Imprimitive Permutation Groups

Edward Dobson
Department of Mathematics and Statistics
Mississippi State University
and
IAM, University of Primorska
dobson@math.msstate.edu

1 Introduction

The O'Nan-Scott Theorem together with the Classification of the Finite Simple Groups is a powerful tool that give the structure of all primitive permutation groups, as well as their actions. This has allowed for the solution to many classical problems, and has opened the door to a deeper understanding of imprimitive permutation groups, as primitive permutation groups are the building blocks of imprimitive permutation groups. We first give a more or less standard introduction to imprimitive groups, and then move to less well-known techniques, with an emphasis on studying automorphism groups of graphs.

A few words about these lecture notes. The lecture notes are an "expanded" version of the lecture - some of the lecture will be basically exactly these lecture notes, but in many cases the proofs of some background results (typically those that in my view are those whose proofs are primarily checking certain computations) are given in these lecture notes but will not be given in the lectures due to time constraints. Also, the material is organized into sections by topic, not by lecture.

2 Basic Results on Imprimitive Groups

Definition 2.1 Let G be a transitive group acting on X. A subset $B \subseteq X$ is a **block** of G if whenever $g \in G$, then $g(B) \cap B = \emptyset$ or B. If $B = \{x\}$ for some $x \in X$ or $B = X$, then B is a **trivial block**. Any other block is nontrivial. If G has a nontrivial block then it is **imprimitive**. If G is not imprimitive, we say that G is **primitive**. Note that if B is a block of G, then $g(B)$ is also a block of B for every $g \in G$, and is called a **conjugate block of** B. The set of all blocks conjugate to B, denoted $\mathcal{B}$, is a partition of X, and $\mathcal{B}$ is called a **complete block system of** G.

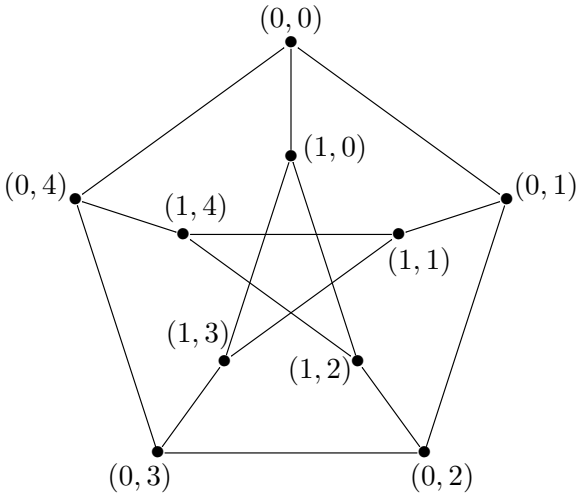
There does not seem to be a standard term for what is called here a complete block system of G. Other authors use a **system of imprimitivity** or a **G-invariant partition** for this term.

Theorem 2.2 *Let $\mathcal{B}$ be a complete block system of G. Then every block in $\mathcal{B}$ has the same cardinality, say k. Further, if m is the number of blocks in $\mathcal{B}$ then mk is the degree of G.*

Theorem 2.3 *Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.*

Proof. Let $x \in X$ and B the orbit of N that contains x, so that $B = \{h(x) : h \in N\}$. Let $g \in G$, and for $h \in N$, denote by h' the element of N such that $gh = h'g$. Note h' always exists as $N \triangleleft G$, and that $\{h' : h \in N\} = N$ as conjugation by g induces an automorphism of N. Then $g(B) = \{gh(x) : h \in N\} = \{h'g(x) : h \in N\} = \{h(g(x)) : h \in N\}$. Hence $g(B)$ is the orbit of N that contains $g(x)$, and as the orbits of N form a partition of X, $g(B) \cap B = \emptyset$ or B. Thus B is a block, and as every conjugate block $g(B)$ of B is an orbit of N, the orbits of N do indeed form a complete block system of G. □

Example 2.4 Define $\rho, \tau : \mathbb{Z}_2 \times \mathbb{Z}_5 \mapsto \mathbb{Z}_2 \times \mathbb{Z}_5$ by $\rho(i, j) = (i, j + 1)$ and $\tau(i, j) = (i + 1, 2j)$. Note that in these formulas, arithmetic is performed modulo 2 in the first coordinate and modulo 5 in the second coordinate. It is straightforward but tedious to check that $\langle \rho, \tau \rangle$ is a subgroup of the automorphism group of the Petersen graph with the labeling shown below:



Additionally, $\tau^{-1}(i, j) = (i - 1, 3j)$ as

$$\tau^{-1}\tau(i, j) = \tau^{-1}(i + 1, 2j) = (i + 1 - 1, 3(2j)) = (i, j).$$

Also,

$$\tau^{-1}\rho\tau(i,j) = \tau^{-1}\rho(i+1,2j) = \tau^{-1}(i+1,2j+1) = (i+1-1,3(2j+1)) = (i,j+3) = \rho^3(i,j)$$

and so $\langle\rho\rangle \triangleleft \langle\rho,\tau\rangle$. Then by Theorem 2.3 the orbits of $\langle\rho\rangle$, which are the sets $\{\{i,j\} : j \in \mathbb{Z}_5\} : i \in \mathbb{Z}_2\}$ form a complete block system of $\langle\rho,\tau\rangle$.

Although we will not show this here, the full automorphism group of the Petersen graph is primitive.

A complete block system of G formed by the orbits of normal subgroup of G is called a **normal complete block system of** G. Note that not every complete block system $\mathcal{B}$ of every transitive group G is a complete block system of G, as we shall see.

Now suppose that $G \leq \mathcal{S}_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k. Then G has an **induced action on** $\mathcal{B}$, which we denote by $G/\mathcal{B}$. Namely, for specific $g \in G$, we define $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$, and set $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. We also define the **fixer of** $\mathcal{B}$ **in** G, denoted $\mathrm{fix}_G(\mathcal{B})$, to be $\{g \in G : g/\mathcal{B} = 1\}$. That is, $\mathrm{fix}_G(\mathcal{B})$ is the subgroup of G which fixes each block of $\mathcal{B}$ set-wise. Furthermore, $\mathrm{fix}_G(\mathcal{B})$ is the kernel of the induced homomorphism $G \to S_{\mathcal{B}}$, and as such is normal in G. Additionally, $|G| = |G/\mathcal{B}| \cdot |\mathrm{fix}_G(\mathcal{B})|$.

A transitive group G is **regular** if $\mathrm{Stab}_G(x) = 1$ for any (and so all) x.

Theorem 2.5 *Let $G \leq \mathcal{S}_n$ be transitive with an abelian regular subgroup H. Then any complete block system of G is normal, and is formed by the orbits of a subgroup of H.*

Proof. We only need show that $\mathrm{fix}_H(\mathcal{B})$ has orbits of size $|B|$, $B \in \mathcal{B}$. Now, $H/\mathcal{B}$ is transitive and abelian, and so $H/\mathcal{B}$ is regular (a transitive abelian group is regular as conjugation permutes the stabilizers of points - so in a transitive abelian group, point stabilizers are all equal). Then $H/\mathcal{B}$ has degree $|\mathcal{B}|$, and so there exists nontrivial $K \leq \mathrm{fix}_H(\mathcal{B})$ of order $|B|$. Then the orbits of K form a complete block system $\mathcal{C}$ of H by Theorem 2.3, and each block of $\mathcal{C}$ is contained in a block of $\mathcal{B}$. As K has order $|B|$, we conclude that $\mathcal{C} = \mathcal{B}$. □

Lemma 2.6 *Let G act transitively on X, and let $x \in X$. Let $H \leq G$ be such that* $\mathrm{Stab}_G(x) \leq H$. *Then the orbit of H that contains x is a block of G.*

Proof. Set $B = \{h(x) : h \in H\}$ (so that B is the orbit of H that contains x), and let $g \in G$. We must show that B is a block of G, or equivalently, that $g(B) = B$ or $g(B) \cap B = \emptyset$. Clearly if $g \in H$, then $g(B) = B$ as B is the orbit of H that contains x and $x \in B$. If $g \notin H$, then towards

a contradiction suppose that $g(B) \cap B \neq \emptyset$, with say $z \in g(B) \cap B$. Then there exists $y \in B$ such that $g(y) = z$ and $h, k \in H$ such that $h(x) = y$ and $k(x) = z$. Then

$$z = g(y) = gh(x) = k(x) = z,$$

and so $gh(x) = k(x)$. Thus $k^{-1}gh \in \mathrm{Stab}_G(x)$. This then implies that $g \in k \cdot \mathrm{Stab}_G(x) \cdot h^{-1} \leq H$, a contradiction. Thus if $g \notin H$, then $g(B) \cap B = \emptyset$, and B is a block of G. □

Example 2.7 Consider the subgroup of the automorphism group of the Petersen graph $\langle \rho\, \tau \rangle$ that we saw before. Straightforward computations will show that $|\tau| = 4$, and so $|\langle \rho, \tau \rangle| = 20$ as $|\rho| = 5$. By the Orbit-Stabilizer Theorem, we have that $\mathrm{Stab}_{\langle \rho,\tau \rangle}(0,0)$ has order 2, and as τ^2 stabilizes $(0,0)$, $\mathrm{Stab}_{\langle \rho,\tau \rangle}(0,0) = \langle \tau^2 \rangle$. Then $\langle \tau \rangle \leq \langle \rho, \tau \rangle$ and contains $\mathrm{Stab}_{\langle \rho,\tau \rangle}(0,0)$. Then the orbit of $\langle \tau \rangle$ that contains $(0,0)$ is a block of $\langle \rho, \tau \rangle$ as well. This orbit is $\{(0,0),(1,0)\}$. So the corresponding complete block system of $\langle \rho, \tau \rangle$ consists of the vertices of the "spoke" edges of the Petersen graph.

Just as we may examine the stabilizer of a point in a transitive group G, we may also examine the **stabilizer of the block** B in an imprimitive group G. It is denoted $\mathrm{Stab}_G(B)$, is a subgroup of G, and $\mathrm{Stab}_G(B) = \{g \in G : g(B) = B\}$.

Theorem 2.8 *Let G act transitively on X, and let $x \in X$. Let Ω be the set of all blocks B of G which contain x, and S be the set of all subgroups $H \leq G$ that contain* $\mathrm{Stab}_G(x)$. *Define $\phi : \Omega \to S$ by $\phi(B) = \mathrm{Stab}_G(B)$. Then ϕ is a bijection, and if $B, C \in \Omega$, then $B \subseteq C$ if and only if* $\mathrm{Stab}_G(B) \leq \mathrm{Stab}_G(C)$.

Proof. First observe that $\mathrm{Stab}_G(x) \leq \mathrm{Stab}_G(B)$ for every block B with $x \in B$, so ϕ is indeed a map from Ω to S. We first show that ϕ is onto. Let $H \in S$ so that $\mathrm{Stab}_G(x) \leq H$. By Lemma 2.6, $B = \{h(x) : h \in H\}$ is a block of G. Then $H \leq \phi(B)$. Towards a contradiction, suppose there exists $g \in \phi(B)$ such that $g \notin H$. Then $g(B) = B$, and H is transitive in its action on B (Exercise 2.12). Hence there exists $h \in H$ such that $h(x) = g(x)$, and so $h^{-1}g(x) = x \in \mathrm{Stab}_G(x) \leq H$. Thus $h^{-1}g \in H$ so $g \in H$, a contradiction. Thus $\phi(B) = H$ and ϕ is onto.

We now show that ϕ is one-to-one. Suppose $B, C \in \Omega$ and $\phi(B) = \phi(C)$. Then $\mathrm{Stab}_G(B) = \mathrm{Stab}_G(C)$. Towards a contradiction, suppose that $y \in B$ but $y \notin C$. As $\mathrm{Stab}_G(B)$ is transitive on B, there exists $h \in \mathrm{Stab}_G(B)$ such that $h(x) = y$. But then $h \in \mathrm{Stab}_G(C) = \mathrm{Stab}_G(B)$ and so y is in the orbit of $\mathrm{Stab}_G(C)$ that contains x, which is C, a contradiction. Thus ϕ is one-to-one and onto, and so a bijection.

Finally, it remains to show that if $B, C \in \Omega$, then $B \subseteq C$ if and only if $\mathrm{Stab}_G(B) \leq \mathrm{Stab}_G(C)$. First suppose that $\mathrm{Stab}_G(B) \leq \mathrm{Stab}_G(C)$. Then the orbit of $\mathrm{Stab}_G(C)$ that contains x certainly

contains the orbit of $\mathrm{Stab}_G(B)$ that contains x, and so $B \subseteq C$. Conversely, suppose that $B \subseteq C$. Let $g \in \mathrm{Stab}_G(B)$. Then $g(x) \in B \subseteq C$, and so $x \in C \cap g(C)$. As C is a block of G, we have that $g(C) = C$ so that $g \in \mathrm{Stab}_G(C)$. Thus $\mathrm{Stab}_G(B) \leq \mathrm{Stab}_G(C)$. □

Theorem 2.9 *Let G be a transitive group acting on X. If $\equiv$ is an equivalence relation on X such that $x \equiv y$ if and only if $g(x) \equiv g(y)$ for all $g \in G$ (a* **G-congruence***), then the equivalence classes of $\equiv$ form a complete block system of G.*

Proof. Let B_x be an equivalence class of $\equiv$ that contains x, and $x \in X$, $g \in G$. Then

$$\begin{aligned} g(B_x) &= \{g(y) : y \in X \text{ and } x \equiv y\} \\ &= \{g(y) : g(y) \equiv g(x)\} \\ &= B_{g(x)}. \end{aligned}$$

As the equivalence classes of $\equiv$ form a partition of X, it follows that $g(B_x) \cap B_x = \emptyset$ or B_x, and so B_x is a block of G. Also, as $g(B_x) = B_{g(x)}$, the set of all blocks conjugate to B_x is just the set of equivalence classes of $\equiv$. □

A common application of the above result is to stabilizers of points, as in a transitive group, any two point stabilizers are conjugate (Exercise ?.?).

Exercise 2.10 *Verify that if B is a block of G, then $g(B)$ is also a block of G for every $g \in G$.*

Exercise 2.11 *Verify that if $\mathcal{B}$ is a complete block system of G acting on X, then $\mathcal{B}$ is a partition of X.*

Exercise 2.12 *Let G act transitively on X, and suppose that B is a block of G. Then $\mathrm{Stab}_G(B)$ is transitive on B.*

Exercise 2.13 *Show that a transitive group of prime degree is primitive.*

Exercise 2.14 *Let $G \leq \mathcal{S}_n$ with $\mathcal{B}$ a complete block system of G. If $\phi \in \mathcal{S}_n$, then $\phi(\mathcal{B})$ is a $\phi G \phi^{-1}$-invariant partition.*

Exercise 2.15 *A group G acting on X is* **doubly-transitive** *if whenever (x_1, y_1), $(x_2, y_2) \in X \times X$ such that $x_1 \neq y_1$ and $x_2 \neq y_2$, then there exists $g \in G$ such that $g(x_1, y_1) = (x_2, y_2)$. Show that a doubly-transitive group is primitive.*

Exercise 2.16 *Let $G \leq \mathcal{S}_n$ contain a regular cyclic subgroup $R = \langle (0\ 1\ \ldots\ n-1)$ and admit a complete block system $\mathcal{B}$ consisting of m blocks of size k. Show that $\mathcal{B}$ consists of cosets of the unique subgroup of $\mathbb{Z}_n$ of order k.*

Exercise 2.17 *Let p and q be distinct primes such that q divides $p-1$. Determine the number of complete block systems of G_L where G is the nonabelian group of order pq that consist of blocks of cardinality q and of cardinality p.*

Exercise 2.18 *Let G be a transitive group of square-free degree (an integer that is* **square-free** *is not divisible by the square of any prime). Show that G has at most one normal G-invariant partition with blocks of prime size p. (Hint: Suppose there are at least two such G-invariant partitions $\mathcal{B}_1$ and $\mathcal{B}_2$. Consider what happens to $\mathrm{fix}_G(\mathcal{B}_2)$ in $G/\mathcal{B}_1$.)*

Exercise 2.19 *Let $G \leq \mathcal{S}_n$ be transitive. Show that G is primitive if and only if $\mathrm{Stab}_G(x)$ is a maximal subgroup of G for every $x \in \mathbb{Z}_n$.*

3 Notions of "sameness" of permutation groups

Definition 3.1 Let $G \leq S_A$ and $H \leq S_B$. Then G and H are **permutation isomorphic** if there exists a bijection $\lambda : A \to B$ and a group isomorphism $\phi : G \to H$ such that $\lambda(g(x)) = \phi(g)(\lambda(x))$ for all $x \in A$ and $g \in G$.

For our discussion of this definition, in which we wish to see that the essential difference between "permutation isomorphic" groups is that the set upon which they act have been relabelled , let's simplify this a bit and assume that $\lambda : A \to A$ is a bijection, and our group isomorphism is the identity. The defining equation then becomes $\lambda(g(x)) = g(\lambda(x))$. The left hand side is what one gets if one applies a group element and then relabels, while the right hand side is what one obtains if one relabels and then applies the group element. So the defining equation says that it doesn't matter if we relabel first and apply group elements or apply group element and then relabel.

Theorem 3.2 *Let G be a transitive group acting on A that admits a complete block system $\mathcal{B}$. Then the action of $\mathrm{Stab}_G(B)$ on B and the action of $\mathrm{Stab}_G(B')$ on B' are permutation isomorphic. Additionally, the action of $\mathrm{fix}_G(\mathcal{B})$ on B is permutation isomorphic to the action of $\mathrm{fix}_G(\mathcal{B})$ on B'.*

Proof. Let $\ell \in G$ such that $\ell(B) = B'$. Define $\lambda : B \to B'$ by $\lambda(x) = \ell(x)$. As ℓ maps B bijectively to B', λ is a bijection. Define $\phi : \mathrm{Stab}_G(B) \to \mathrm{Stab}_G(B')$ by $\phi(g) = \ell g \ell^{-1}$. As ϕ is obtained by conjugation, ϕ is a group isomorphism. Let $g \in \mathrm{Stab}_G(B)$, and $x \in B$. Then

$$\lambda(g(x)) = \ell g(x) = \ell g \ell^{-1} \ell(x) = \phi(g)\lambda(x),$$

and so the action of $\mathrm{Stab}_G(B)$ on B is permutation isomorphic to the action of $\mathrm{Stab}_G(B')$ on B'. Analogous arguments will show that the action of $\mathrm{fix}_G(\mathcal{B})$ on B is permutation isomorphic to the action of $\mathrm{fix}_G(\mathcal{B})$ on B'. □

There is another notion of "sameness" for permutation groups, as we may not only relabel the set on which the group acts, but relabel the group elements (via a group automorphism).

Definition 3.3 We say that $G \leq S_A$ and $H \leq S_B$ are **permutation equivalent** if there exists a bijection $\lambda : A \to B$, $\alpha \in \mathrm{Aut}(G)$, and a group isomorphism $\phi : G \to H$ such that $\lambda(\alpha(g)(x)) = \phi(g)(\lambda(x))$ for all $x \in A$ and $g \in G$.

As before, for our discussion, let's assume that $A = B$ and $\phi = 1$. In fact, in most cases, permutation equivalence is *only* defined in this manner. The defining equation then becomes $\lambda(\alpha(g)(x)) = g\lambda(x)$. The left hand side of this equation says to relabel the group element and apply to x, and then relabel the set. The right hand side says to relabel the set, then apply g. As these are equal, this essentially says that relabeling the group is the same as relabeling the set.

Notice that if $\alpha = 1$, then the definition of permutation equivalence and permutation isomorphism are the same. In general, as

$$\lambda(g(x)) = \lambda(\alpha(\alpha^{-1}(g))(x)) = \phi(\alpha^{-1}(g)(\lambda(x)) = (\phi\alpha^{-1})(g)(\lambda(x)),$$

for all $\alpha^{-1}(g) \in G$, we have the following result.

Lemma 3.4 *If $G \leq S_A$ and $H \leq S_B$ are permutation equivalent, then G and H are permutation isomorphic.*

Proof. Suppose that G and H are permutation equivalent so that there exists $\lambda : A \to B$, $\alpha \in \mathrm{Aut}(G)$, and $\phi : G \to H$ an isomorphism such that $\lambda(\alpha(g)(x)) = \phi(g)(\lambda(x))$ for all $x \in A$ and $g \in G$. Then

$$\begin{aligned} \lambda(g(x)) &= \lambda(\alpha(\alpha^{-1}(g))(x)) \\ &= \phi(\alpha^{-1}(g)(\lambda(x)) \\ &= (\phi\alpha^{-1})(g)(\lambda(x)). \end{aligned}$$

for all $x \in A$ and $g \in G$. □

It is usual to state a result characterizing when transitive actions of a group G acting on sets A and B are equivalent. By "a group G acting on sets A and B" it is meant that $\alpha = 1$. In other words, we look at the action of an element of G on the two different sets, and do not allow "relabeling" of the group (as that formally changes the group element). Indeed, some authors only define the equivalence "equivalence of permutation groups" in this way.

Theorem 3.5 *Let G act transitively on A and B. Then the action of G on A is equivalent to the action of G on B if and only if the stabilizer in G of a point in A is the stabilizer of a point in B.*

PROOF. Suppose that the action of G on A is equivalent to the action of G on B. Then there exists a bijection $\lambda : A \to B$ such that $\lambda(g(x)) = g(\lambda(x))$ for all $x \in A$ and $g \in G$. Let $K = \mathrm{Stab}_G(z)$, where $z \in B$, and $y \in A$ such that $\lambda(y) = z$. Let $k \in K$. As $k(z) = z$, we have that

$$\lambda(k(y)) = k(\lambda(y)) = k(z) = z.$$

As λ is a bijection, $k(y) = \lambda^{-1}(z) = y$, and so k stabilizes y. Thus $K \leq \mathrm{Stab}_G(y)$, and as G is transitive on A and B and $|A| = |B|$, by the Orbit-Stabilizer Theorem we see that $K = \mathrm{Stab}_G(y)$.

Now suppose that $\mathrm{Stab}_G(a) = \mathrm{Stab}_G(b)$ for some $a \in A$ and $b \in B$. Define $\lambda : A \mapsto B$ by $\lambda(g(a)) = g(b)$. We first need to show that λ is well-defined. That is, that regardless of choice of g, $\lambda(x) = y$, $x \in A$, $y \in B$, is the same. So we need to show that if $g(a) = h(a)$, then $g(b) = \lambda(g(a)) = \lambda(h(a)) = h(b)$. Now,

$$\begin{aligned} g(a) = h(a) &\Rightarrow h^{-1}g(a) = a \\ &\Rightarrow h^{-1}g \in \mathrm{Stab}_G(a) \\ &\Rightarrow h^{-1}g(b) = b \\ &\Rightarrow g(b) = h(b) \\ &\Rightarrow \lambda(g(a)) = \lambda(h(a)) \end{aligned}$$

and so λ is indeed well-defined. Also, as G is transitive on A, λ has domain A, and as G is transitive on B, λ is surjective, and hence bijective. Finally, let $x \in A$. Then there exists $h_x \in G$ such that $h_x(a) = x$. Then

$$\begin{aligned} \lambda(g(x)) &= \lambda(gh_x(a)) \\ &= gh_x(b) \\ &= g\lambda(h_x(a)) \\ &= g\lambda(x). \end{aligned}$$

□

4 An Example of Inequivalent Actions: The Automorphism Group of the Heawood Graph

For a subspace S of $\mathbb{F}_q^n$, we denote by $S^\perp$ the **othogonal complement of S**. That is, $S^\perp = \{w \in \mathbb{F}_q^n : w \cdot v = 0 \text{ for every } v \in S\}$. Recall that $S^\perp$ is a subspace of the vector space $\mathbb{F}_q^n$. A **line** in $\mathbb{F}_q^n$ is a one-dimensional subspace, while a **hyperplane** is the orthogonal complement of a line (so a subspace of $\mathbb{F}_q^n$ of dimension $n-1$). Note that the number of lines and hyperplanes of $\mathbb{F}_q^n$ are the same. In the case of $\mathbb{F}_2^3$ which contains 8 elements, any nonzero vector gives rise to a line, so there are 7 lines and 7 hyperplanes.

Consider the graph whose vertex set is the lines and hyperplanes of $\mathbb{F}_2^3$, and a line is adjacent to a hyperplane if and only if the line is contained in the hyperplane. We obtain the following graph, which is isomorphic to the Heawood graph:

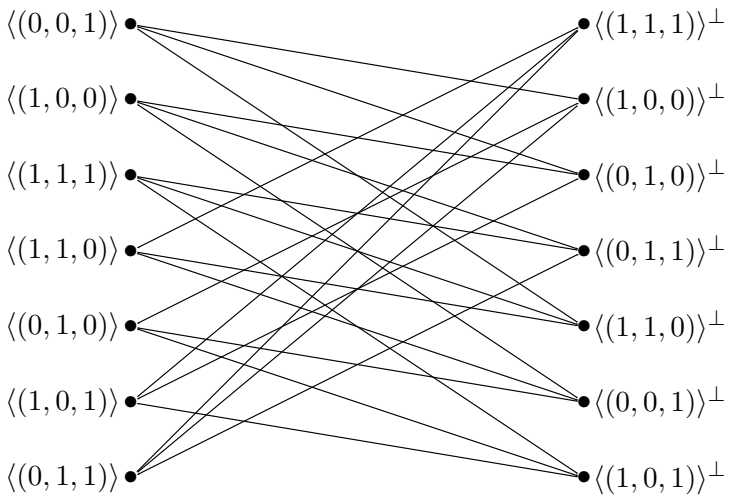


Figure 1: The Heawood graph labeled with the lines and hyperplanes of $\mathbb{F}_2^3$

Recall that $\mathrm{GL}(n, \mathbb{F}_q)$ is the **general linear group of dimension n over the field $\mathbb{F}_q$**. That is $\mathrm{GL}(n, \mathbb{F}_q)$ is the group of all invertible $n \times n$ matrices with entries in $\mathbb{F}_q$, with binary operation multiplication. In the literature, it is common to see $\mathrm{GL}(n, q)$ written in place of $\mathrm{GL}(n, \mathbb{F}_q)$, a convention that we will follow. Of course, a linear transformation maps lines to lines, so we can consider the action of $\mathrm{GL}(3, 2)$ on the lines of $\mathbb{F}_2^3$, and obtain the group $\mathrm{PGL}(3, 2)$, which is isomorphic to $\mathrm{GL}(3, 2)$. Note that $\mathrm{PGL}(3, 2)$ also permutes the hyperplanes of $\mathbb{F}_2^3$. Of course, an

element of $\mathrm{PGL}(3,2)$ maps a line contained in a hyperplane to a line contained in a hyperplane, and so $\mathrm{PGL}(3,2)$ is contained in $\mathrm{Aut}(\mathrm{Hea})$, where Hea is the Heawood graph. Notice that $\mathrm{PGL}(3,2)$ is transitive on the lines of $\mathbb{F}_2^3$ and transitive on the hyperplanes of $\mathbb{F}_2^3$.

Now define $\tau : L \cup H \to L \cup H$ by $\tau\{\ell, h\} = \{h^\perp, \ell^\perp\}$. Note that τ is well-defined, as the subspace orthogonal to a line is a hyperplane, while the subspace orthogonal to a hyperplane is a line. Clearly $|\tau| = 2$ as $(s^\perp)^\perp = s$. In order to show that $\tau \in \mathrm{Aut}(\mathrm{Hea})$, let $\ell \in L$ and $h \in H$ such that $\ell \subset h$. Then every vector in $h^\perp$ is orthogonal to every vector in h, and as $\ell \subset h$, every vector in $h^\perp$ is orthogonal to every vector in ℓ. Thus $h^\perp \subset \ell^\perp$ and so if $\ell h \in E(\mathrm{Hea})$, then $\tau(\ell h) \in E(\mathrm{Hea})$. Thus $\tau \in \mathrm{Aut}(H)$.

Lemma 4.1 *Let $g \in \mathrm{GL}(n,q)$, and s a subspace of $\mathbb{F}_q^n$. Then $g(s^\perp)^\perp = (g^{-1})^T(s)$.*

Proof. First recall that if $w, v \in \mathbb{F}_q^n$, then the dot product of w and v, $w \cdot v$, can also be written as $w^T v$, where for a matrix g, g^T denotes the transpose of g. Let $w_1, \ldots, w_r$ be a basis for $s^\perp$, so that $g(s^\perp)$ has basis $gw_1, \ldots, gw_r$. In order to show that $g(s^\perp)^\perp = (g^{-1})^T(s)$, it suffices to show that $(g^{-1})^T v$ is orthogonal to gw_i for any i and $v \in s$ as $\dim(s) + \dim(s^\perp) = n$. Then

$$(gw_i) \cdot (g^{-1})^T v = (gw_i)^T (g^{-1})^T v = w_i^T g^T (g^{-1})^T v = w_i^T v = 0.$$

□

Consider the canonical action of $\mathrm{PGL}(3,2)$ on $L \cup H$, so that $g \in \mathrm{PGL}(3,2)$, then $g(\ell, h) = \{g(\ell), g(h)\}$. Now, let $g \in \mathrm{PGL}(3,2)$, which will consider in the above action on $L \cup H$. Then

$$\begin{aligned} \tau^{-1} g \tau(\{\ell, h\}) &= \tau^{-1} g(\{h^\perp, \ell^\perp\}) \\ &= \tau^{-1}(\{g(h^\perp), g(\ell^\perp)\}) \\ &= \{g(\ell^\perp)^\perp, g(h^\perp)^\perp\} \\ &= \{(g^{-1})^T(\ell), (g^{-1})^T(h)\} \end{aligned}$$

Then $\tau^{-1} g \tau = g^{-1})^T$ so $\mathrm{PGL}(3,2) \triangleleft \langle \mathrm{PGL}(3,2), \tau \rangle$.

Now, $\langle \mathrm{PGL}(3,2), \tau \rangle$ admits a complete block system $\mathcal{B}$ with 2 blocks of size 7. The subgroup of $\mathrm{PGL}(3,2)$ that stabilizes a line does not stabilize any hyperplane! So we have that $\mathrm{PGL}(3,2)$ acts inequivalently on the lines and hyperplanes. It can be shown using a theorem of Tutte that $\mathrm{Aut}(\mathrm{Hea}) = \langle \mathrm{PGL}(3,2), \tau \rangle$.

5 The Embedding Theorem

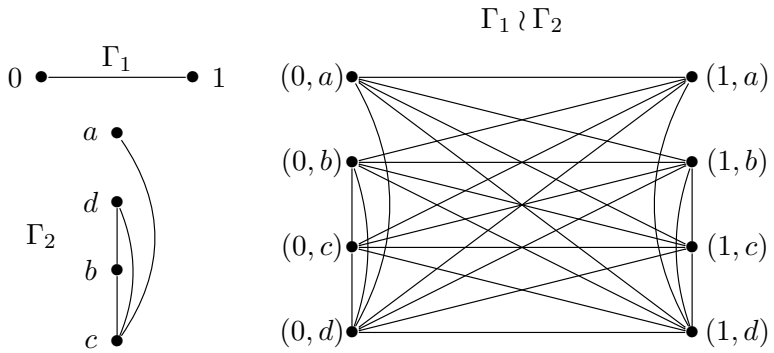
Definition 5.1 Let Γ_1 and Γ_2 be digraphs. The **wreath product of** Γ_1 **and** Γ_2, denoted $\Gamma_1 \wr \Gamma_2$ is the digraph with vertex set $V(\Gamma_1) \times V(\Gamma_2)$ and edge set

$$\{(u,v)(u,v') : u \in V(\Gamma_1) \text{ and } vv' \in E(\Gamma_2)\} \cup \{(u,v)(u',v') : uu' \in E(\Gamma_1) \text{ and } v, v' \in V(\Gamma_2)\}.$$

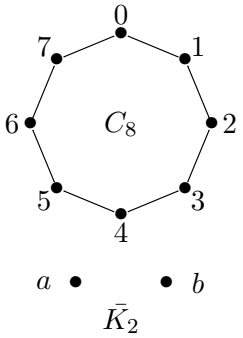
Intuitively, $\Gamma_1 \wr \Gamma_2$ is constructed as follows. First, we have $|V(\Gamma_1)|$ copies of the digraph Γ_2, with these $|V(\Gamma_1)|$ copies indexed by elements of $V(\Gamma_1)$. Next, between corresponding copies of Γ_2 we place every possible directed from one copy to another if in Γ_1 there is an edge between the indexing labels of the copies of Γ_2, and no edges otherwise.

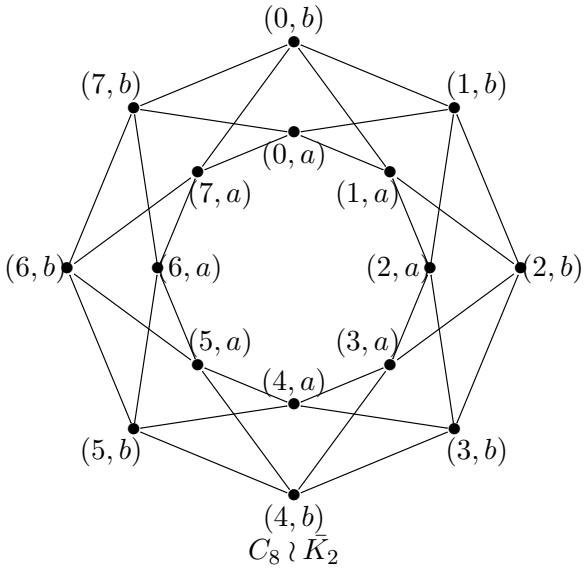
To find the wreath product of any two graphs Γ_1 and Γ_2:

1. First corresponding to each vertex of Γ_1, put a copy of Γ_2.
2. If v_1 and v_2 are adjacent in Γ_1, put every edge between corresponding copies of Γ_2.



Let us consider the graph $C_8 \wr \bar{K}_2$.





$C_8 \wr \bar{K}_2$

In the previous graph, think of the sets $\{(i, j) : j \in \mathbb{Z}_2\}$ as blocks. Take any automorphism of C_8, and think of it as "permuting" the blocks. A block is mapped to a block by any automorphism of $\bar{K}_2$, and we can have different automorphisms of $\bar{K}_2$ for different blocks. This is the group $\mathrm{Aut}(C_8) \wr \mathrm{Aut}(\bar{K}_2)$.

Definition 5.2 Let G be a permutation group acting on X and H a permutation group acting on Y. Define the **wreath product of G and H**, denoted $G \wr H$, to be the set of all permutations of $X \times Y$ of the form $(x, y) \to (g(x), h_x(y))$.

Definition 5.3 Let G be a transitive permutation group acting on X that admits a complete block system $\mathcal{B}$. Then the action of G on $\mathcal{B}$ induces a permutation group in $S_{\mathcal{B}}$, which we denote by $G/\mathcal{B}$. More specifically, if $g \in G$, then define $g/\mathcal{B} : \mathcal{B} \to \mathcal{B}$ by $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$, and set $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$.

Theorem 5.4 *Let G be a transitive permutation group acting on X that admits a complete block system $\mathcal{B}$. Then G is permutation isomorphic to a subgroup of $(G/\mathcal{B}) \wr (\mathrm{Stab}_G(\mathcal{B})|_{B_0})$, where $B_0 \in \mathcal{B}$.*

Proof. For each $B \in \mathcal{B}$, there exists h_B such that $h_B(B_0) = B$. Define $\lambda : X \to \mathcal{B} \times B_0$ by $\lambda(x) = (B, x_0)$, where $x \in B$ and $x_0 = h_B^{-1}(x)$. Define $\phi : G \to (G/\mathcal{B}) \wr (\mathrm{Stab}_G(\mathcal{B})|_{B_0})$ by $\phi(g)(B, x_0) = (g(B), h_{g(B)}^{-1} g h_B(x_0))$. We must show that λ is a bijection, ϕ is an injective homomorphism, and that $\lambda(g(x)) = \phi(g)(\lambda(x))$ for all $x \in X$ and $g \in G$.

In order to show that λ is a bijection, it suffices to show that λ is one-to-one as by Theorem 2.2 it is certainly the case that $|X| = |\mathcal{B} \times B_0|$. Let $x, x' \in X$ and assume that $(B, x_0) = \lambda(x) = \lambda(x')$.

Clearly then both x and x' are contained in B, and $x_0 = h_B^{-1}(x) = h_B^{-1}(x')$. As h_B is a permutation, it follows that $x = x'$ and λ is one-to-one and so a bijection.

To show that ϕ is injective, suppose that $\phi(g) = \phi(g')$. Applying the definition of ϕ, we see that

$$(g(B), h_{g(B)}^{-1} g h_B(x_0)) = (g'(B), h_{g'(B)}^{-1} g' h_B(x_0)),$$

for all $B \in \mathcal{B}$ and $x_0 \in B_0$. It immediately follows that $g/\mathcal{B} = g'/\mathcal{B}$ and $h_{g(B)}^{-1} g h_B = h_{g'(B)}^{-1} g' h_B$. Using the fact that $g/\mathcal{B} = g'/\mathcal{B}$ and canceling, we see that $g = g'$ and ϕ is injective.

Let $g_1, g_2 \in G$. Then

$$\begin{aligned}
\phi(g_1)\phi(g_2)(B, x_0) &= \phi(g_1)(g_2(B), h_{g_2^{-1}(B)} g_2 h_B(x_0)) \\
&= (g_1 g_2(B), h_{g_1(g_2(B))}^{-1} g_1 h_{g_2(B)} (h_{g_2(B)}^{-1} g_2 h_B(x_0)) \\
&= (g_1 g_2(B), h_{g_1 g_2(B)}^{-1} g_1 g_2 h_B(x_0)) \\
&= \phi(g_1 g_2)(B, x_0),
\end{aligned}$$

and so ϕ is a homomorphism.

Finally, observe that $\phi(g)(\lambda(x)) = \phi(g)(B, x_0) = (g(B), h_{g(B)}^{-1} g h_B(x_0))$ while

$$\lambda(g(x)) = (g(B), h_{g(B)}^{-1} g(x)) = (g(B), h_{g(B)}^{-1} g h_B(x_0)),$$

and so $\lambda(g(x)) = \phi(g)(\lambda(x))$ for all $x \in X$ and $g \in G$. □

The following immediate corollary is often useful.

Corollary 5.5 *Let G be a transitive permutation group that admits a complete block system $\mathcal{B}$ consisting of m blocks of size k. Then G is permutation isomorphic to a subgroup of $S_m \wr S_k$.*

One must be slightly careful with this labeling, as it is not always the most natural labeling. For example, let q and p be prime with $q|(p-1)$ and $\alpha \in \mathbb{Z}_p^*$ of order q. Define $\rho, \tau : \mathbb{Z}_q \times \mathbb{Z}_p \mapsto \mathbb{Z}_q \times \mathbb{Z}_p$ by $\tau(i, j) = (i + 1, \alpha j)$ and $\rho(i, j) = (i, j + 1)$. Then $\langle \rho, \tau \rangle$ is isomorphic to the nonabelian group of order qp. The labeling that one would get for this group by applying the Embedding Theorem is $\langle \rho', \tau' \rangle$, where $\rho'(i, j) = (i, j + \alpha^i)$, $\tau'(i, j) = (i + 1, j)$.

6 A graph theoretic tool

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a

p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle (here $\gamma|_B$ is the induced permutation of g on B). It is straightforward to verify that $\equiv$ is an equivalence relation (Exercise 6.2). Let C be an equivalence class of $\equiv$ and $E_C = \cup_{B \in C} B$ (remember that the equivalence classes of $\equiv$ consist of *blocks* of $\mathcal{B}$), and $\mathcal{E} = \{E_C : C \text{ is an equivalence class of } C\}$.

Lemma 6.1 *Let Γ be a digraph with $G \leq \mathrm{Aut}(\Gamma)$ admit a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Let $\equiv$ and $\mathcal{E}$ be defined as in the preceding paragraph. Then $\mathcal{E}$ is a complete block system of G and for every $g \in \mathrm{fix}_G(\mathcal{B})$, $g|_E \in \mathrm{Aut}(\Gamma)$ for every $E \in \mathcal{E}$. Here $g|_E(x) = g(x)$ if $x \in E$ while $g(x) = x$ if $x \notin E$.*

Proof. We will first show that $\mathcal{E}/\mathcal{B}$ is a complete block system of $G/\mathcal{B}$ by showing that $\equiv$ is a $G/\mathcal{B}$-congruence and applying Theorem 2.9. This will then imply that $\mathcal{E}$ is a complete block system of G. We thus need to show that if $B \equiv B'$ and $g \in G$, then $g(B) \equiv g(B')$ for every $g \in G$. Suppose that $g(B) \not\equiv g(B')$. Then there exists $\gamma \in \mathrm{fix}_G(\mathcal{B})$ such that $\gamma|_{g(B)}|_B$ is a p-cycle but $\gamma|_{g(B')}$ is not a p-cycle. Let $b \in B$. Then $g^{-1}\gamma g(b) = g^{-1}\gamma(g(b))$ and so $g^{-1}\gamma g|_B$ is a p-cycle, while a similar argument shows that $g^{-1}\gamma g|_B$ is not. We conclude that if $B \equiv B'$ then $g(B) \equiv g(B')$ and so $\mathcal{E}$ is indeed a complete block system of G.

Now suppose that $B \not\equiv B'$. We will first show that in Γ, either every vertex of B is our or in adjacent to every vertex of B', or there is no edge between any vertex of B and any vertex of B'. So, suppose that there is an edge from say B to B'. As $B \not\equiv B'$, there is $\gamma \in \mathrm{fix}_G(\mathcal{B})$ such that $\gamma|_B$ is a p-cycle while $\gamma|_{B'}$ is not a p-cycle. Raising γ to the power $|\gamma|_{B'}|$ which is relatively prime to γ, we may assume without loss of generality that $\gamma|_{B'} = 1$. Let the directed edge $b_0\vec{b'} \in E(\Gamma)$, where $b_0 \in B$ and $b' \in B'$. As $\gamma|_B$ is a p-cycle, we may write $\gamma|_B = (b_0\ b_1\ \ldots\ b_{p-1})$ (i.e. we are writing $\gamma|_B$ as a p-cycle starting at b_0). Applying γ to the edge $b_0\vec{b'}$, we obtain the edge $b_1\vec{b'}$, and applying γ to the edge $b_0\vec{b'}$ r times, we obtain the edge $b_r\vec{b'}$. We conclude that $b\vec{b'} \in E(\Gamma)$ for every $b \in B$. Now, there exists $\delta \in \mathrm{fix}_G(\mathcal{B})$ such that $\delta|_{B'}$ is a p-cycle. Applying δ to each of the edges $b\vec{b'}$ $p-1$ times (similar to above), we have that the edges $b\vec{b'} \in E(\Gamma)$ for every $b \in B$ and $b' \in \mathcal{B}$. Similar arguments will show that if $b'\vec{b} \in E(\Gamma)$ for some $b' \in B'$ and $b \in B$, then $b'\vec{b} \in E(\Gamma)$ for every $b' \in B'$ and $b \in B$, as well as if $bb' \in E(\Gamma)$ for some $b, b' \in E(\Gamma)$, then $bb' \in E(\Gamma)$ for all $b \in B$ and $b' \in B'$.

Now, let $\gamma \in \mathrm{fix}_G(\mathcal{B})$, and consider the map $\gamma|_E$, $E \in \mathcal{E}$. If $e = x\vec{y} \in E(\Gamma)$ and both $x, y \in E$, then surely $\gamma|_E(e) = \gamma(e) \in E(\Gamma)$. Similarly, if both $x, y \notin E$, then $\gamma|_E(e) = e \in E(\Gamma)$. If $x \in E$ but $y \notin E(\Gamma)$, then let $B_x, B_y \in \mathcal{B}$ such that $x \in B_x$ and $y \in B_y$. Then $x'\vec{y'} \in E(\Gamma)$ for every $x' \in B_x$, $y' \in B_y$ by arguments above. Also, $\gamma(x) = x' \in B_x$, and so $\gamma|_E(e) = x'\vec{y} \in E(\Gamma)$. An analogous argument will show that $\gamma|_E(e) \in E(\Gamma)$ if $x \notin E$ but $y \in E$. As in every case, $\gamma|_E \in E(\Gamma)$, we have that $\gamma|_E \in \mathrm{Aut}(\Gamma)$ establishing the result. □

The above result also holds in the more general situation that $\mathrm{fix}_G(\mathcal{B})$ acts primitively on $B \in \mathcal{B}$.

Exercise 6.2 *Write a careful proof that $\equiv$ is an equivalence relation.*

7 Basic definitions concerning graphs

Definition 7.1 Let G be a group and $S \subset G$. Define a **Cayley digraph of** G, denoted $\mathrm{Cay}(G, S)$ to be the graph with $V(\mathrm{Cay}(G, S)) = G$ and $E(\mathrm{Cay}(G, S)) = \{(g, gs) : g \in G, s \in S\}$. We call S the **connection set of** $\mathrm{Cay}(G, S)$.

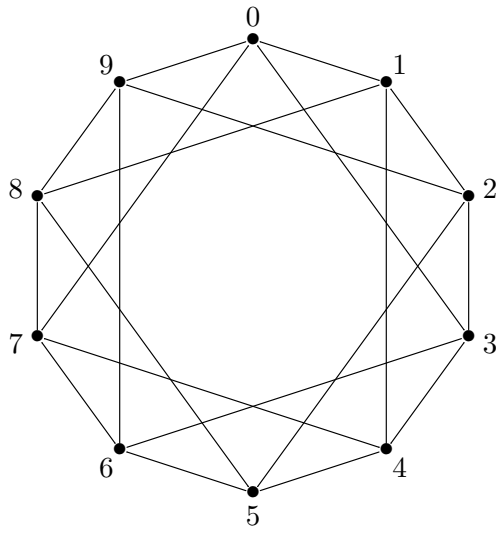


Figure 2: The Cayley graph $\mathrm{Cay}(\mathbb{Z}_{10}, \{1, 3, 7, 9\})$.

If we additionally insist that $S = S^{-1} = \{s^{-1} : s \in S\}$ (or if the group is abelian and the operation is addition, that $S = -S$), then there will be no directed edges in $\mathrm{Cay}(G, S)$, and we obtain a **Cayley graph**. This follows as if $(g, gs) \in E(\mathrm{Cay}(G, S))$ and $s^{-1} \in S$, then $(gs, gs(s^{-1})) = (gs, s) \in E(\mathrm{Cay}(G, S))$. In many situations, whether or not a Cayley digraph has loops doesn't have any effect. In these cases the default is usually to exclude loops by also insisting that $1_G \notin S$ (or $0 \notin S$ if G is abelian and the operation is addition).

Perhaps the most common Cayley digraphs that one encounters are Cayley digraphs of the cyclic groups $\mathbb{Z}_n$ of order n, as in Figure 2. A Cayley (di)graph of $\mathbb{Z}_n$ is called a **circulant** (di)graph of order n.

Definition 7.2 For a group G, the **left regular representation** , denoted G_L , is the subgroup of S_G given by the left translations of G. More specifically, $G_L = \{x \to gx : g \in G\}$. We denote

the map $x \to gx$ by g_L. It is straightforward to verify that G_L is a group and that $G_L \cong G$.

Let $x, y \in G$, and $g = yx^{-1}$. Then $g_L(x) = yx^{-1}x = y$ so that G_L is transitive on G.

Lemma 7.3 *For every $S \subseteq G$, $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$.*

PROOF. Let $e = (g, gs) \in E(\mathrm{Cay}(G, S)$, where $g \in G$ and $s \in S$. Let $h \in G$. We must show that $h_L(e) \in E(\mathrm{Cay}(G, S))$, or that $h_L(e) = (g', g's')$ for some $g' \in G$ and $s' \in S$. Setting $g' = hg$ and $s' = s$, we have that

$$h_L(e) = h_L(g, gs) = (hg, h(gs)) = (hg, (hg)s) = (g', g's').$$

□

In general, for an abelian group G, the group G_L will consist of "translations by g" that map $x \to x + g$. That is, $G_L = \{x \to x + g : g \in G\}$. More specifically, for a cyclic group $\mathbb{Z}_n$, we have that $\mathbb{Z}_n$ is generated by the map $x \to x + 1$ (or course instead on 1, one could put any generator of $\mathbb{Z}_n$).

The following important result of G. Sabidussi [8] characterizes Cayley graphs.

Theorem 7.4 *A graph Γ is isomorphic to a Cayley graph of a group G if and only if* $\mathrm{Aut}(\Gamma)$ *contains a regular subgroup isomorphic to G.*

PROOF. If $\Gamma \cong \mathrm{Cay}(G, S)$ with $\phi : \Gamma \to \mathrm{Cay}(G, S)$ an isomorphism, then by Lemma 7.3, $\mathrm{Aut}(\mathrm{Cay}(G, s))$ contains the regular subgroup $G_L \cong G$, namely $\phi^{-1} G_L \phi$ (see Exercise 7.6). Conversely, suppose that $\mathrm{Aut}(\Gamma)$ contains a regular subgroup $H \cong G$, with $\omega : H \to G$ an isomorphism. Fix $v \in V(\Gamma)$. As H is regular, for each $u \in V(\Gamma)$, there exists a unique $h_u \in H$ such that $h_u(v) = u$. Define $\phi : V(\Gamma) \to G$ by $\phi(u) = \omega(h_u)$. Note that as each h_u is unique, ϕ is well-defined and is also a bijection as ω is a bijection. Let $U = \{u \in V(\Gamma) : (v, u) \in E(\Gamma)\}$. We claim that $\phi(\Gamma) = \mathrm{Cay}(G, \phi(U))$.

As $\phi(V(\Gamma)) = G$, $V(\phi(\Gamma)) = G$. Let $e \in E(\phi(\Gamma))$. We must show that $e = (g, gs)$ for some $g \in G$ and $s \in \phi(U)$. As $e \in E(\phi(\Gamma))$, $\phi^{-1}(e) = (u_1, u_2) \in E(\Gamma)$ by Exercise 7.6. Let $w \in V(\Gamma)$ such that $h_{u_1}(w) = u_2$. Then $h_{u_1}^{-1}(u_1, u_2) = (v, w)$ so that $w = h_w(v) \in U$, and $h_{u_2} = h_{u_1} h_w$ as $h_{u_1} h_w(v) = h_{u_1}(w) = u_2$. Thus

$$(u_1, u_2) = (h_{u_1}(v), h_{u_1}(w)) = (h_{u_1}(v), h_{u_1} h_w(v)) = (h_{u_1}(v), h_{u_2}(v)).$$

Set $g = \omega(h_{u_1})$ and $s = \omega(h_w)$. Then

$$\phi(u_1, u_2) = (\omega(h_{u_1}), \omega(h_{u_2})) = (\omega(h_{u_1}), \omega(h_{u_1} h_w)) = (\omega(h_{u_1}), \omega(h_{u_1})\omega(h_w)) = (g, gs)$$

as required. □

We now prove a well-known result first proven by Turner [10].

Theorem 7.5 *Every transitive group of prime degree p contains a cyclic regular subgroup. Consequently, every vertex-transitive digraph is isomorphic to a circulant digraph of order p.*

PROOF. Let G be a transitive group of prime degree p. As G is transitive, it has one orbit of size p, and so p divides $|G|$. Hence G has an element of order p, which is necessarily a p-cycle permuting all of the points. So G contains a regular cyclic subgroup, and the result follows by Theorem 7.4. □

Exercise 7.6 *Show that if $\phi : \Gamma \to \Gamma'$ is a graph isomorphism, then $\phi^{-1} : \Gamma' \to \Gamma$ is also a graph isomorphism. Then show that if $H \leq \mathrm{Aut}(\Gamma')$, then $\phi^{-1} H \phi \leq \mathrm{Aut}(\Gamma)$.*

8 An application to graphs

Definition 8.1 Let m and n be positive integers, and $\alpha \in \mathbb{Z}_n^*$. Define $\rho, \tau : \mathbb{Z}_m \times \mathbb{Z}_n \mapsto \mathbb{Z}_m \times \mathbb{Z}_n$ by $\rho(i, j) = (i, j+1)$ and $\tau(i, j) = (i+1, \alpha j)$. A vertex-transitive Γ digraph with vertex set $\mathbb{Z}_m \times \mathbb{Z}_n$ is an (m, n)**-metacirculant digraph** if and only if $\langle \rho, \tau \rangle \leq \mathrm{Aut}(\Gamma)$.

The Petersen graph is a $(2, 5)$-metacirculant graph with $\alpha = 2$, while the Heawood graph is a $(2, 7)$-metacirculant graph with $\alpha = 6$.

Lemma 8.2 *Let $\rho : \mathbb{Z}_m \times \mathbb{Z}_n \mapsto \mathbb{Z}_m \times \mathbb{Z}_n$ by $\rho(i, j) = (i, j + 1)$. Then $Z_{S_{mn}}(\langle \rho \rangle) = \{(i, j) \mapsto (\sigma(i), j + b_i) : \sigma \in S_n, b_i \in \mathbb{Z}_n\} = S_m \wr (\mathbb{Z}_n)_L$.*

PROOF. Straightforward computations will show that every element of $\{(i, j) \mapsto (\sigma(i), j + b_i)$ does indeed centralize $\langle \rho \rangle$. Then $Z_{S_{mn}}(\langle \rho \rangle)$ is transitive as $\rho \in Z_{S_{mn}}(\langle \rho \rangle)$. Additionally, $\langle \rho \rangle \lhd Z_{S_{mn}}(\langle \rho \rangle)$, and so the orbits $\mathcal{B}$ of $\langle \rho \rangle$ form a complete block system of $Z_{S_{mn}}(\langle \rho \rangle)$. Let $B \in \mathcal{B}$, and $g \in \mathrm{Stab}_{Z_{S_{mn}}(\langle \rho \rangle)}(B)$. Then $g|_B$ commutes with $\langle \rho \rangle|_B$, and as $\langle \rho \rangle|_B$ is a regular cyclic group, it is self-centralizing (we have already seen that a transitive abelian group is regular in the proof of Theorem 2.5. The subgroup generated by any element that centralizes a regular abelian group and the regular abelian group is a transitive abelian group, and so regular.) Then $\mathrm{Stab}_{Z_{S_{mn}}(\langle \rho \rangle)}(B)|_B \leq \langle \rho \rangle|_B$, and

so by the Embedding Theorem 5.4, $Z_{S_{mn}}(\langle\rho\rangle) \leq S_m \wr (\mathbb{Z}_n)_L$. As $S_m \wr (\mathbb{Z}_n)_L \leq Z_{S_{mn}}(\langle\rho\rangle)$, the result follows. □

Theorem 8.3 *A vertex-transitive digraph Γ of order qp, q and p distinct primes, is isomorphic to a (q,p)-metacirculant digraph if and only if* $\mathrm{Aut}(\Gamma)$ *has a transitive subgroup G that contains a normal complete block system $\mathcal{B}$ with q blocks of size p.*

Proof. If Γ is isomorphic to a (q,p)-metacirculant, then after an appropriate relabeling, $\langle\rho,\tau\rangle \leq \mathrm{Aut}(\Gamma)$. Then $\langle\rho\rangle \lhd \langle\rho,\tau\rangle = G$ has orbits of length p.

Conversely, suppose that there exists $N \lhd G \leq \mathrm{Aut}(\Gamma)$ and N has orbits of length p. Let $\mathcal{B}$ be the complete block system formed by the orbits of N, and assume that G is the largest subgroup of $\mathrm{Aut}(\Gamma)$ that admits $\mathcal{B}$. Then $G/\mathcal{B}$ is transitive, and so G contains an element τ such that $\langle\tau\rangle/\mathcal{B}$ is cyclic of order q (and so regular), and τ has order a power of q. By Lemma 6.1 there exists $\rho \in G$ such that $\langle\rho\rangle$ is semiregular of order p, and a Sylow p-subgroup P of $\mathrm{fix}_G(\mathcal{B})$ has order p or p^q. If $|P| = p^q$, then if there is a directed edge in Γ from some vertex of B to some vertex of B', $B, B' \in \mathcal{B}$, then there is a directed edge from every vertex of B to every vertex of B'. We conclude that Γ is isomorphic to a wreath product of vertex-transitive digraphs of order q and p, respectively, and so by Theorem 7.5, Γ is isomorphic to the wreath product of a circulant digraph of order q and a circulant digraph of order p. By Exercise 8.4, Γ is isomorphic to a Cayley digraph of $\mathbb{Z}_q \times \mathbb{Z}_p$, and every such digraph is isomorphic to a (q,p)-metacirculant digraph by Exercise 8.5. We henceforth assume that $|P| = p$.

Now, $\langle\rho\rangle$ and $\tau^{-1}\langle\rho\rangle\tau$ are contained in Sylow p-subgroups P_1 and P_2 of $\mathrm{fix}_G(\mathcal{B})$, respectively, and so there exists $\delta \in G$ such that $\delta^{-1}P_2\delta = P_1$. Replacing τ with $\tau\delta$, if necessary, we assume without loss of generality that $\tau^{-1}\langle\rho\rangle\tau \leq P_1$. As $|P_1| = |P_2| = p$, we see that $\tau^{-1}\langle\rho\rangle\tau = \langle\rho\rangle$. We now label the vertex set of Γ with elements of $\mathbb{Z}_q \times \mathbb{Z}_p$ in such a way that $\rho(i,j) = (i, j+1)$, and $\tau(i,j) = (i+1, \omega_i(j))$, where $\omega_i \in S_p$, $i \in \mathbb{Z}_q$. Set $\tau^{-1}\rho\tau = \rho^a$, where $a \in \mathbb{Z}_p^*$. Define $\bar{a} : \mathbb{Z}_q \times \mathbb{Z}_p \to \mathbb{Z}_q \times \mathbb{Z}_p$ by $\bar{a}(i,j) = (i, aj)$. Then $\bar{a}^{-1}\rho^a\bar{a} = \rho$. Then $\tau\bar{a}$ centralizes $\langle\rho\rangle$, and so by Lemma 8.2, we see that $\tau\bar{a} \in \{(i,j) \mapsto (\sigma(i), j + b_i) : \sigma \in S_q, b_i \in \mathbb{Z}_p\}$. We conclude that $\tau\bar{a}(i,j) = (i+1, j+b_i)$, $b_i \in \mathbb{Z}_p$, and so $\tau(i,j) = (i+1, a^{-1}j + c_i)$, $c_i \in \mathbb{Z}_p$.

Let $H = \langle\tau, z_k : k \in \mathbb{Z}_q\rangle$, where $z_k(i,j) = (i, j + \delta_{ik})$, where δ_{ik} is Kronecker's delta function. That is $\delta_{ik} = 1$ if $i = k$ and 0 otherwise. Note that $\langle z_k : k \in \mathbb{Z}_q\rangle \lhd H$ and $H/\langle z_k : k \in \mathbb{Z}_q\rangle \cong \langle\tau\rangle$. We conclude that $\langle\tau\rangle$ is a Sylow q-subgroup of H. Now let, $\tau' : \mathbb{Z}_q \times \mathbb{Z}_p \mapsto \mathbb{Z}_q \times \mathbb{Z}_p$ by $\tau'(i,j) = (i+1, a^{-1}j)$. Then $\tau' \in H$ and also has order $|\tau|$, and so $\langle\tau'\rangle$ is a Sylow q-subgroup of H as well. Thus there exists $\gamma \in H$ such that $\gamma^{-1}\langle\tau\rangle\gamma = \langle\tau'\rangle$. Also, $\langle\rho\rangle \lhd H$, and so $\gamma^{-1}\langle\rho\rangle\gamma = \langle\rho\rangle$, and so $\gamma^{-1}\langle\rho,\tau\rangle\gamma = \langle\rho,\tau'\rangle$. Then Γ is isomorphic to a (q,p)-metacirculant digraph. □

Exercise 8.4 *Show that for any two groups G and H, $G_L \wr H_L$ contains a regular subgroup isomorphic to $G \times H$. Deduce that the wreath product of two Cayley digraphs is a Cayley digraph.*

Exercise 8.5 *Let n be a positive integer and $n = mk$, where $\gcd(m,k) = 1$. Show that any circulant digraph of order n is isomorphic to an (m,k)-metacirculant digraph.*

9 A general strategy for analyzing imprimitive permutation groups with blocks of prime size - especially automorphism groups of vertex-transitive digraphs

Let G be a transitive group that admits a complete block system $\mathcal{B}$ with blocks of prime size p. If $\mathcal{B}$ is not a normal complete block system, then $G/\mathcal{B}$ is a transitive faithful representation of G, so hopefully one can use induction... Otherwise, $\mathcal{B}$ is normal. If $\mathrm{fix}_G(\mathcal{B})$ is not faithful on $B \in \mathcal{B}$, then in the general case, one cannot say much about $\mathrm{fix}_G(\mathcal{B})$ other than the normalizer of a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ is a vector space invariant under its normalizer, which is transitive. Tools from linear algebra may be employed - not promising but not hopeless either. In the case of the automorphism group of a vertex-transitive graph, one may employ Lemma 6.1 in which case the Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has a very restrictive structure as we have seen. If $\mathrm{fix}_G(\mathcal{B})$ is faithful on $B \in \mathcal{B}$ there are three cases to consider. The first is when $\mathrm{fix}_G(\mathcal{B}) \cong \mathbb{Z}_p$. This is the most difficult case to deal with, and nothing more will be said of this case now. If $\mathrm{fix}_G(\mathcal{B}) \neq \mathbb{Z}_p$, then there are two subcases, depending on whether or not the action of $\mathrm{fix}_G(\mathcal{B})$ on $B, B' \in \mathcal{B}$ are always equivalent or if the are inequivalent. We now investigate this...

Lemma 9.1 *Let $G \leq S_n$ be transitive on V and admit a normal complete block system $\mathcal{B}$ with blocks of size p. Suppose that $\mathrm{fix}_G(\mathcal{B}) \neq \mathbb{Z}_p$ is faithful on $B \in \mathcal{B}$. Define an equivalence relation $\equiv$ on V by $v_1 \equiv v_2$ if and only if $\mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(v_1) = \mathrm{Stab}_{\mathrm{fix}_G(\mathcal{B})}(v_2)$. Then the equivalence classes of $\equiv$ are blocks of G, and each equivalence class of $\equiv$ contains at most one point of $B \in \mathcal{B}$.*

Proof. As conjugation by an element of G maps the stabilizer of a point in $\mathrm{fix}_G(\mathcal{B})$ to the stabilizer of a point in $\mathrm{fix}_G(\mathcal{B})$, $\equiv$ is a G-congruence, and so by Theorem 2.9 the equivalence classes of $\equiv$ are blocks of G. If a block contains two points from the same equivalence class, then by first part of this lemma applied to $\mathrm{fix}_G(\mathcal{B})|_B$, we see that $\mathrm{fix}_G(\mathcal{B})|_B$ is imprimitive. But a transitive group of prime degree is primitive, a contradiction. □

Let $\mathcal{E}$ be the complete block system consisting of the equivalence classes of $\equiv$ in the previous lemma. Suppose that each equivalence class of $\equiv$ contains exactly one element of each $B \in \mathcal{B}$. This means that $|B \cap E| = 1$ for every $B \in \mathcal{B}$ and $E \in \mathcal{E}$. Two complete $\mathcal{B}$ and $\mathcal{C}$ of G such that

$|B \cap C| = 1$ for every $B \in \mathcal{B}$ and $C \in \mathcal{C}$ are called **orthogonal complete block systems**. Observe that if $\mathcal{B}$ and $\mathcal{C}$ are orthogonal and $\mathcal{B}$ consists of m blocks of size k, then $\mathcal{C}$ consists of k blocks of size m.

Lemma 9.2 *Let $n = mk$ and $G \leq S_n$ such that G is transitive and admits orthogonal complete block systems $\mathcal{B}$ and $\mathcal{C}$ of m blocks of size k and k blocks of size m, respectively. Then G is permutation equivalent to a subgroup of $S_k \times S_m$ in its natural action on $\mathbb{Z}_k \times \mathbb{Z}_m$.*

PROOF. Note that G has a natural action on $\mathcal{B} \times \mathcal{C}$ given by $g(B, C) = (g(B), g(C))$, and that in this action each $g \in G$ induces a permutation contained in $S_{\mathcal{B}} \times S_{\mathcal{C}}$, namely, $(g/\mathcal{B}, g/\mathcal{C})$. Any element of G in the kernel of this representation of G must fix every block of $\mathcal{B}$ and every block of $\mathcal{C}$. As $|B \cap C| = 1$ for every $B \in \mathcal{B}$ and $C \in \mathcal{C}$, and there are exactly $mk = n$ such intersections, the kernel of this representation is the identity and the representation is faithful. Let $B \in \mathcal{B}$ and $C \in \mathcal{C}$. If $g \in G$ stabilizes the point (B, C) in this representation, then $g(B) = B$ and $g(C) = C$. Let $B \cap C = \{x\}$. Then $g(x) = x$. Conversely, if $g(x) = x$, then there exists $B \in \mathcal{B}$ and $C \in \mathcal{C}$ such that $x \in B$ and $x \in \mathcal{C}$. Then $g(B, C) = (B, C)$ so $\mathrm{Stab}_G(x) = \mathrm{Stab}_G((B, C))$. It then follows by Theorem 3.5 that these two actions of G are equivalent. □

Combining the two previous lemmas we have:

Lemma 9.3 *Let $G \leq S_n$ be transitive on V and admit a normal complete block system $\mathcal{B}$ with blocks of size p. Suppose that $\mathrm{fix}_G(\mathcal{B}) \neq \mathbb{Z}_p$ is faithful on $B \in \mathcal{B}$. If the action of $\mathrm{fix}_G(\mathcal{B})$ on B and B' are always equivalent, then G is permutation isomorphic to a subgroup of $S_{n/p} \times S_p$.*

We now illustrate these techniques by calculating the full automorphism group of circulant digraphs of order p^2, where p is prime.

Theorem 9.4 *Let Γ be a circulant digraph of order p^2, p an odd prime. Then one of the following is true:*

- $(\mathbb{Z}_{p^2})_L \triangleleft \mathrm{Aut}(\Gamma)$, *or*
- $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma_1) \wr \mathrm{Aut}(\Gamma_2)$ *where, Γ_1 and Γ_2 are circulant digraphs of prime order, or*
- $\Gamma = K_{p^2}$ *or its complement and* $\mathrm{Aut}(\Gamma) = S_{p^2}$.

Note: The result is simpler if $p = 2$, and as $|S_4| = 24$, everything can be easily determined by hand.

PROOF. A **Burnside group** is a group G with the property that whenever $H \leq S_n$ contains G as a regular subgroup, then either H is doubly-transitive or H is imprimitive. Here, H is doubly-transitive if whenever we have two order pairs (x_1, y_1) and (x_2, y_2) with $x_1 \neq y_1$ and $x_2 \neq y_2$, then there exists $h \in H$ such that $h(x_1, y_1) = (x_2, y_2)$. Schur showed that a cyclic group of composite order is a Burnside group [2, Theorem 3.5A]. So $\mathrm{Aut}(\Gamma)$ is either imprimitive or doubly-transitive. If $\mathrm{Aut}(\Gamma)$ is doubly-transitive, then Γ is either K_{p^2} or its complement and the result follows. Otherwise, $\mathrm{Aut}(\Gamma)$ admits a complete block system $\mathcal{B}$ consisting of p blocks of size p. (In the case $\mathbb{Z}_q \times \mathbb{Z}_p$, we still have a Burnside group, while for $\mathbb{Z}_p \times \mathbb{Z}_p$, the possibilities for a simply primitive group are given explicitly by the O'Nan-Scott Theorem.)

Let $\rho : \mathbb{Z}_{p^2} \mapsto \mathbb{Z}_{p^2}$ by $\rho(i) = i + 1 \pmod{p^2}$, so that $\langle \rho \rangle$ is a regular subgroup of $\mathrm{Aut}(\Gamma)$ of order p^2. $\mathcal{B}$ is then necessarily normal, and formed by the orbits of a normal subgroup of $\langle \rho \rangle$ of order p. There is a unique such subgroup, namely $\langle \rho^p \rangle$. Consider the equivalence relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle. By Lemma 6.1, the union of the equivalence classes of $\equiv$ form a complete block system $\mathcal{E}$, and $\rho^p|_E \in \mathrm{Aut}(\Gamma)$ for every $E \in \mathcal{E}$. If $\mathcal{E}$ has blocks of size p, then $\mathcal{E} = \mathcal{B}$, and Γ is isomorphic to the wreath product of two circulant digraphs of prime order. A result of Sabidussi [9] then gives (2).

If $\mathcal{E}$ consists of one block of size p^2, then $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})$ acts faithfully on $B \in \mathcal{B}$ as otherwise, as a normal subgroup of a primitive group is necessarily transitive, the kernel K of the action of $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})$ on $B \in \mathcal{B}$ is transitive on some $B' \in \mathcal{B}$, and so K has order divisible by p. Then K contains an element which is a p-cycle on B' and the identity on B, and so $B \not\equiv B'$. We first consider when $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{B}) \ncong \mathbb{Z}_p$.

We now wish to apply a famous result of Burnside which states that a transitive group of prime degree is either permutation isomorphic to a subgroup of $\mathrm{AGL}(1, p) = \{x \mapsto ax+b : a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p\}$, or is a doubly-transitive group with nonabelian socle. A consequence of the Classification of the Finite Simple groups is that all doubly-transitive groups are known [1, Table], and then one can show (by examining each possible case), that a doubly-transitive group either has 1 or 2 inequivalent representations. If $H \leq \mathrm{AGL}(1, p)$ is transitive and not isomorphic to $\mathbb{Z}_p$ (note that p will divide $|H|$), then $|H| = ap$, $a > 1$. Then $\mathrm{Stab}_H(x)$ has order a, and as $\mathrm{AGL}(1, p)$ is solvable of order $p(p-1)$, H is solvable and $\gcd(a, p) = 1$. By Hall's Theorem, any two subgroups of order a are conjugate in H. We conclude by Theorem 3.5 that H has a unique representation of degree p.

Now define an equivalence relation $\equiv'$ on $\mathbb{Z}_{p^2}$ by $i \equiv j$ if and only if $\mathrm{Stab}_{\mathrm{fix}_{\mathrm{Aut}(\Gamma)}}(i) = \mathrm{Stab}_{\mathrm{fix}_{\mathrm{Aut}(\Gamma)}}(j)$. Note that as $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})$ is primitive on $B \in \mathcal{B}$, no equivalence class of $\equiv'$ can contain more than one element of $B \in \mathcal{B}$. If there is a unique representation of $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})$ as a transitive group of degree p, then the equivalence classes of $\equiv'$ form an orthogonal complete block system of $\mathrm{Aut}(\Gamma)$.

However, as $\mathbb{Z}_{p^2}$ contains a unique subgroup of order p and every complete block system is normal, there is no such orthogonal complete block system, a contradiction! (Note that if $\mathbb{Z}_{p^2}$ is replaced with $\mathbb{Z}_p \times \mathbb{Z}_p$ of $\mathbb{Z}_q \times \mathbb{Z}_p$, there is no contradiction, but we still are done as then $\mathrm{Aut}(\Gamma)$ is contained in a direct product and it is easy to figure out what happens). We thus assume that $\mathrm{fix}_G(\mathcal{B}) \cong \mathbb{Z}_p$.

Of course $\mathrm{Aut}(\Gamma)/\mathcal{B}$ is a transitive group of prime degree, so by Burnside's Theorem it is either contained in $\mathrm{AGL}(1,p)$ or is a doubly-transitive group with nonabelian socle. If $\mathrm{Aut}(\Gamma)/\mathcal{B} \leq \mathrm{AGL}(1,p)$, then as $\mathrm{AGL}(1,p)$ contains a normal Sylow p-subgroup which is necessarily $\langle\rho\rangle/\mathcal{B}$, we see that $\langle\rho\rangle \lhd \mathrm{Aut}(\Gamma)$ and the result follows. I will not really talk about the other case - it doesn't really have much to do with imprimitive groups, and is also the hardest case. I will say that in the case under consideration, this cannot occur, while if $q \neq p$ it not only can occur, but in fact has two different outcomes. For $\mathbb{Z}_p \times \mathbb{Z}_p$ it also can occur but only has the obvious outcome of being something like $H \times \mathbb{Z}_p$, where $H \leq S_p$. □

10 Further Reading

Extensions of Burnside's Theorem to transitive groups of degree p^2 as well as the full automorphism groups of all vertex-transitive digraphs of order p^2 can be found in [5]. An extension of Burnside's Theorem for transitive groups that contain a regular cyclic group of prime-power order can be found in [3]. An extension of Burnside's Theorem for groups that contain a regular abelian Hall π-subgroup is in [6]. Some information about transitive groups of degree qp can be found in [4], together with the full automorphism groups of all vertex-transitive graphs of order qp. An extension of Burnside's Theorem for a regular semidirect product of two cyclic groups of prime-power degree can be found in [7] (we remark that while the results in this paper are stated only for graphs, the graph structure is not used much - so the result is not explicitly stated, but can be extracted).

References

[1] Peter J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), no. 1, 1–22. MR MR599634 (83m:20008) 21

[2] John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996. MR MR1409812 (98m:20003) 21

[3] Edward Dobson, *On groups of odd prime-power degree that contain a full cycle*, Discrete Math. **299** (2005), no. 1-3, 65–78. MR MR2168696 (2006j:20004) 22

[4] ———, *Automorphism groups of metacirculant graphs of order a product of two distinct primes*, Combin. Probab. Comput. **15** (2006), no. 1-2, 105–130. MR MR2195578 (2006m:05108) 22

[5] Edward Dobson and Dave Witte, *Transitive permutation groups of prime-squared degree*, J. Algebraic Combin. **16** (2002), no. 1, 43–69. MR MR1941984 (2004c:20007) 22

[6] Li Cai-Heng Dobson, Edward and Pablo Spiga, *Permutation groups containing a regular abelian hall subgroup*, Comm. Algbr. **40** (2012), 3532–3539. 22

[7] Cai Heng Li and Hyo-Seob Sim, *On half-transitive metacirculant graphs of prime-power order*, J. Combin. Theory Ser. B **81** (2001), no. 1, 45–57. MR 1809425 (2002m:05106) 22

[8] Gert Sabidussi, *On a class of fixed-point-free graphs*, Proc. Amer. Math. Soc. **9** (1958), 800–804. MR MR0097068 (20 #3548) 16

[9] ———, *The composition of graphs*, Duke Math. J **26** (1959), 693–696. MR MR0110649 (22 #1524) 21

[10] James Turner, *Point-symmetric graphs with a prime number of points*, J. Combinatorial Theory **3** (1967), 136–145. MR MR0211908 (35 #2783) 17