On transitive ternary relational structures of order a prime-squared

Edward Dobson
Department of Mathematics and Statistics
Mississippi State University
PO Drawer MA Mississippi State, MS 39762
dobson@math.msstate.edu

Abstract

We determine the full Sylow p-subgroup of the automorphism group of transitive k-ary relational structures of order p^2, p a prime. We then find the full automorphism group of transitive ternary relational structures of order p^2, for those values of p for which A_p is the only doubly-transitive nonabelian simple group of degree p. Finally, we determine optimal necessary and sufficient conditions for two Cayley k-ary relational structures of order p^2, $k < p$, to be isomorphic.

1 Introduction

We begin by finding the full Sylow p-subgroup of the automorphism group of transitive k-ary relational structures of order p^2 (Corollary 3.4). Using this result as well as results of the author and D. Witte in [8], we determine the full automorphism group of transitive ternary relational structures of order p^2, for those values of p for which A_p is the only doubly-transitive nonabelian simple group of degree p (Theorems 3.10 and 3.11). Using the characterization of the full Sylow p-group of the automorphism groups of k-ary relational structures, we also give optimal necessary and sufficient conditions for two Cayley k-ary relational structures of order p^2 to be isomorphic (Theorems 3.5 and 3.6). While this problem only forms a part of this paper, the remainder of the introduction will focus on putting the results on the isomorphism problem into perspective, as quite a bit of work (references are provided below) has been done on this problem for the groups under consideration in this paper.

ARS COMBINATORIA 97A(2010), pp. 15-32

Modern interest in the isomorphism problem under consideration in this paper began in 1967 when Ádám [1] conjectured that two circulant graphs of order n are isomorphic if and only if they are isomorphic by a group automorphism of $\mathbb{Z}_n$. Subsequently, Ádám's original conjecture was generalized in several directions. First, a circulant graph is just a Cayley graph of $\mathbb{Z}_n$, so one obvious generalization of Ádám's conjecture is to ask for which groups G is it true that any two Cayley graphs of G are isomorphic if and only if they are isomorphic by a group automorphism of G?

Definition 1.1 Let G be a group. If two Cayley graphs of G are isomorphic if and only if they are isomorphic by a group automorphism of G, we say that G is a CI-group with respect to graphs.

Much work on this problem has been done, and the interested reader is referred to [13] for a recent survey of results on this problem. Another obvious generalization is to ask the same question about different combinatorial objects. That is, given a class $\mathcal{K}$ of Cayley objects, for which groups G is it true that if X and X' are Cayley objects of G in $\mathcal{K}$ are X and X' isomorphic if and only if they are isomorphic by a group automorphism of G?

Definition 1.2 Let X be an object in some class $\mathcal{K}$ of combinatorial objects. We say that X is a Cayley object of G if $V(X) = G$ and $G_L = \{x \to gx : g \in G\}$ is a subgroup of $\mathrm{Aut}(X)$.

Definition 1.3 Let G be a group and $\mathcal{K}$ a class of combinatorial objects. If two Cayley objects of G in $\mathcal{K}$ of G are isomorphic if and only if they are isomorphic by a group automorphism of G, we say that G is a CI-group with respect to $\mathcal{K}$.

Pálfy [16] has shown that a group G is a CI-group with respect to every class of combinatorial objects if and only if $\gcd(n, \varphi(n)) = 1$ or $n = 4$ where φ is Euler's phi function. He also showed that if G is not a CI-group with respect to some class of combinatorial objects, then G is not a CI-group with respect to 4-ary relational structures. This implies that for "most" classes $\mathcal{K}$ of combinatorial objects, "most" groups G are not CI-groups with respect to $\mathcal{K}$. But for those classes $\mathcal{K}$ and groups G, we still have the problem of determining necessary and sufficient conditions for two Cayley objects of G in $\mathcal{K}$ to be isomorphic. This problem is sometimes referred to as the Cayley isomorphism problem.

Recently, there have been several results published in the literature along the lines of Pálfy's theorem mentioned above. Namely, an explicit list of permutations have been given for a group G, and two Cayley objects of the group G in some class of combinatorial objects are isomorphic if and

only if they are isomorphic by some permutation on the given list. This has been accomplished for $G = \mathbb{Z}_{pq}$ [10], $\mathbb{Z}_{p^2}$ [11] (another, later proof can be found in [8]), and $\mathbb{Z}_p^2$ [8], where p and q are distinct primes. Results like these certainly solve the Cayley isomorphism problem for all classes $\mathcal{K}$ of combinatorial objects, but for a specific class of combinatorial object, it need not be the most efficient condition. For example, the number of permutations that need to be checked to determine if two Cayley objects of $\mathbb{Z}_p^2$ given by [8] is at least $(p^2-1)(p^2-p)+(p-2)(p-1)(p^2-1)(p^2-p)$, but Godsil has shown [9], that $\mathbb{Z}_p^2$ is a CI-group with respect to graphs, so that only $(p^2-p)(p^2-1)$ permutations need to be checked for graphs. Thus, though the results cited above are powerful, they do not produce a *minimal* list of permutations to be checked to determine isomorphism within a specific class of combinatorial objects. In this paper, we will determine such a minimal list for k-ary relational structures of an abelian group of order p^2, p a prime with $k < p$. We remark that these are natural classes of combinatorial objects to consider (they include k-uniform hypergraphs, for example), as a result of Wielandt [18, Theorem 5.12] (this hard to find reference can be found in it's entirety in [19]) implies that every transitive group is the automorphism group of some k-ary relational structure.

2 Preliminaries

For permutation group terminology not given in this paper, see [7]. We begin with a well-known and useful result by Burnside.

Theorem 2.1 (Burnside, [4]) *Let G be a transitive group of prime degree. Then either G is doubly transitive or G contains a normal Sylow p-subgroup.*

As all doubly-transitive groups are known (see [5]), the above result determines all transitive groups of degree p, p a prime. The author and Witte [8] have determined all transitive group of degree p^2, p a prime, with some explicit exceptions. In particular, if p is a prime such that A_p and S_p are the only nonsolvable doubly-transitive groups of degree p, then [8] explicitly constructs all transitive groups of degree p^2. We shall have need of this result, as well as some of the results used to prove this.

Definition 2.2 Let G be a transitive permutation group of degree mp acting on $\mathbb{Z}_m \times \mathbb{Z}_p$ that admits a complete block system $\mathcal{B}$ of m blocks of cardinality p. If $g \in G$, then g permutes the m blocks of $\mathcal{B}$ and hence induces a permutation in S_m denoted $g/\mathcal{B}$. We define $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$, and let $\mathrm{fix}_G(\mathcal{B}) = \{g \in G : g(B) = B \text{ for every } B \in \mathcal{B}\}$.

Definition 2.3 Let G be a transitive permutation group of degree mp acting on $\mathbb{Z}_m \times \mathbb{Z}_p$. Assume that $\mathrm{fix}_G(\mathcal{B}) \neq 1$ so that a Sylow p-subgroup P_0 of $\mathrm{fix}_G(\mathcal{B})$ is nontrivial. Define $z_i: \mathbb{Z}_m \times \mathbb{Z}_p \to \mathbb{Z}_m \times \mathbb{Z}_p$ by $z_i(j,k) = (j,k)$ if $j \neq i$ and $z_i(j,k) = (j, k+1)$ if $j = i$. Without loss of generality, assume that P_0 is contained in $\langle z_i : i \in \mathbb{Z}_m \rangle$. For $h \in P_0$, we then have that $h = \prod_{i=0}^{m-1} z_i^{a_i}$, $a_i \in \mathbb{Z}_p$. Define $v: P_0 \to Z_p^m$ by $v(h) = (a_0, a_1, \ldots, a_{m-1})$.

With the above definitions in hand, we have the following result.

Lemma 2.4 (Lemma 3, [8]) *If there exists $x \in G$ such that $x(i,j) = (i+1, \alpha j + b_i)$, $b_i \in \mathbb{Z}_p$, $\alpha \in \mathbb{Z}_p^*$, then $\{v(h) : h \in P_0\}$ is a cyclic code of length m over $GF(p)$. Conversely, if C is a cyclic code of length m over $GF(p)$, then there exists a group G as above such that $P_0 = \{ \prod_{i=0}^{m-1} z_i^{a_i} : (a_0, a_1, \ldots, a_{m-1}) \in C \}$.*

Definition 2.5 The code of Lemma 2.4 will be denoted by $C_{\mathcal{B}}$, and will be called the code induced by $\mathcal{B}$. If G admits a unique block system $\mathcal{B}$ of m blocks of cardinality p, we say $C_{\mathcal{B}}$ is the code over $GF(p)$ *induced* by G.

We will have need of the permutational wreath product of two groups.

Definition 2.6 Let $G \leq S_X$ and $H \leq S_Y$. We define the (permutational) wreath product of G and H, denoted $G \wr H$, to be the group of all permutations in $S_{X \times Y}$ of the form $(x,y) \to (g(x), h_x(y))$, where $g \in G$ and each $h_x \in H$.

Definition 2.7 Let $a_{i,j} = \binom{i}{j}(-1)^{i-j}$. A straightforward calculation will show that $a_{i,j-1} = a_{i+1,j} + a_{i,j}$. For $1 \leq i \leq p$, let

$$\gamma_i = z_0^{a_{p-i,0}} z_1^{a_{p-i,1}} \cdots z_{p-1}^{a_{p-i,p-1}}.$$

Define $\tau: \mathbb{Z}_{p^2} \to \mathbb{Z}_{p^2}$ by

$$\tau(i) = i + 1 (\mathrm{mod}\ p^2)$$

and $\rho_1, \rho_2: \mathbb{Z}_p^2 \to \mathbb{Z}_p^2$ by

$$\rho_1(i,j) = (i, j+1) \text{ and } \rho_2(i,j) = (i+1, j)$$

We remark that we may also view z_i as acting on $\mathbb{Z}_{p^2}$, in which case $z_i(a + bp) = a + bp$ if $a \neq i$ and $z_i(a+bp) = a + (b+1)p$ if $a = i$. Let

$$P_i = \langle \tau, \gamma_i \rangle \text{ and } P_i' = \langle \rho_1, \rho_2, \gamma_i \rangle,$$

for $1 \leq i \leq p$. We remark that $P_p = P_p' \cong \mathbb{Z}_p \wr \mathbb{Z}_p$. There are thus $2p-1$ distinct groups P_i, P_i', $1 \leq i \leq p$.

Theorem 2.8 (Theorem 9, [8]) *Let G be a transitive group of degree p^2 with Sylow p-subgroup P. Let $|P| = p^{i+1}$, $i \geq 1$.*

- *If $\tau \in P$, then $P = P_i$.*
- *If $\langle \rho_1, \rho_2 \rangle \leq P$, then $P = \alpha^{-1} P_i' \alpha$ for some $\alpha \in \mathrm{Aut}(\mathbb{Z}_p^2)$.*

It is not difficult to show (see [8]) that every transitive group of degree p^2 contains a regular subgroup (so permutation isomorphic to $\langle \tau \rangle$ or $\langle \rho_1, \rho_2 \rangle$). Thus the above result gives, up-to permutation isomorphism, all Sylow p-subgroups of a transitive group of degree p^2. The following result characterizes when a transitive p-subgroup of S_{p^2} contains regular subgroups isomorphic to both $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p^2$.

Lemma 2.9 (Lemma 4, [8]) *Let P be a transitive p-subgroup of S_{p^2}. Then P admits a complete block system $\mathcal{B}$ of p blocks of cardinality p.*
Furthermore, the following are equivalent:

1. *P does not contain regular copies of both $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p^2$.*
2. *$P \ncong \mathbb{Z}_p \wr \mathbb{Z}_p$.*
3. *Letting C be the code induced by $\mathcal{B}$, we have $\sum_{i=0}^{p-1} a_i \equiv 0 \pmod{p}$, for every $(a_0, a_1, \ldots, a_{p-1}) \in C$.*

The following result gives all transitive groups of degree p^2 whose Sylow p-subgroup is not a full Sylow p-subgroup of S_{p^2} (which is $\mathbb{Z}_p \wr \mathbb{Z}_p$).

Theorem 2.10 (Theorem 4, [8]) *Let G be a transitive group of degree p^2 such that a Sylow p-subgroup P of G is not isomorphic to $\mathbb{Z}_p \wr \mathbb{Z}_p$. Then, after replacing G by a conjugate, one of the following is true.*

1. *G is doubly transitive, and either*
   - *$G = A_{p^2}$ or S_{p^2}; or*
   - *$\mathrm{PSL}(n,k) \leq G \leq \mathrm{P\Gamma L}(n,k)$, where $(k^n - 1)/(k-1) = p^2$; or*
   - *$\mathbb{Z}_p \times \mathbb{Z}_p \leq G \leq \mathrm{AGL}(2,p)$.*
2. *G is simply primitive, has an elementary abelian Sylow p-subgroup and either*
   - *$\mathbb{Z}_p \times \mathbb{Z}_p \leq G \leq \mathrm{AGL}(2,p)$; or*
   - *G has a transitive, imprimitive subgroup H of index 2, such that $H \leq S_p \times S_p$ (H is described in [8, Lemma 1]),*

3. *G is imprimitive, $P \ncong \mathbb{Z}_p \times \mathbb{Z}_p$, $P \ncong P'_{p-1}$, and $P \lhd G$, so $P \leq G \leq N_{S_{p^2}}(P)$ (and $N_{S_{p^2}}(P)$ is described in [8, Lemma 5] or [8, Lemma 6]);*

4. *G is imprimitive, $P = \mathbb{Z}_p \times \mathbb{Z}_p$ and $G \leq S_p \times S_p$ (G is described in [8, Lemma 1]); or*

5. *G is imprimitive, $P = P'_{p-1}$, and $G = LP$, where $\mathbb{Z}_p \times \mathbb{Z}_p \leq L \leq S_p \times \mathrm{AGL}(1,p)$ (L is described in [8, Lemma 1]).*

Remark 2.11 *We remark that in the preceding result, if $\mathrm{PSL}(n,k) \leq G \leq \mathrm{P\Gamma L}(n,k)$, where $(k^n-1)/(k-1) = p^2$, then G contains a regular cyclic subgroup but does not contains a subgroup isomorphic to $\mathbb{Z}_p^2$, while if $\mathbb{Z}_p \times \mathbb{Z}_p \leq G \leq \mathrm{AGL}(2,p)$, then G contains a regular subgroup isomorphic to $\mathbb{Z}_p^2$ but does not contains a regular cyclic subgroup.*

Definition 2.12 ([6, p. 168]) Let H be a group and let A be an H-module. (That is, A is an abelian group on which H acts by automorphisms.) A function $\phi\colon H \to A$ is a *crossed homomorphism* if, for every $h_1, h_2 \in H$, we have

$$\phi(h_1 h_2) = h_2^{-1} \cdot \phi(h_1) + \phi(h_2).$$

(This is equivalent to the assertion that the function $H \to H \ltimes A$ defined by $h \mapsto (h, \phi(h))$ is a homomorphism.)

The following result characterizes all transitive groups of degree p^2 that have Sylow p-subgroup isomorphic of $\mathbb{Z}_p \wr \mathbb{Z}_p$.

Proposition 2.13 (Proposition 1, [8]) *Let*

1. *p be a prime;*

2. *H and L be transitive subgroups of S_p, such that L is simple;*

3. *K/L^p be an H-invariant subgroup of the abelian group $\left(N_{S_p}(L)/L\right)^p$;*

4. *$\phi\colon H \to N_{S_p}(L)^p/K$ be a crossed homomorphism; and*

5. *$G_{H,L,K,\phi} = \{\, (h,v) \in H \ltimes N_{S_p}(L)^p : \phi(h) = vK \,\} \leq S_p \wr S_p$.*

Then $G_{H,L,K,\phi}$ is a transitive, imprimitive subgroup of S_{p^2}, such that a Sylow p-subgroup of G is isomorphic to $\mathbb{Z}_p \wr \mathbb{Z}_p$.

Conversely, if G is a transitive, imprimitive permutation group of degree p^2, such that a Sylow p-subgroup of G is isomorphic to $\mathbb{Z}_p \wr \mathbb{Z}_p$, then G is equivalent to $G_{H,L,K,\phi}$, for some H, L, K, and ϕ as above.

Definition 2.14 (cf. [6, Prop. 4.1]) Let H be a group, let A be an H-module, and let $\phi_1, \phi_2 \colon H \to A$ be crossed homomorphism. We say that ϕ_1 is *cohomologous* to ϕ_2 if there is an element a of A, such that, for every $h \in H$, we have

$$\phi_1(h) - \phi_2(h) = h^{-1}a - a.$$

(This is equivalent to the assertion that the homomorphisms $h \mapsto (h, \phi_1(h))$ and $h \mapsto (h, \phi_2(h))$ are conjugate via an element of A.)

We remark that the equivalence classes of this equivalence relation are, by definition, the elements of the cohomology group $H^1(H, A)$.

Theorem 2.15 (Theorem 13, [8]) *Let*

- *p be a prime;*
- *H be either A_p, S_p, or subgroup of $\mathrm{AGL}(1,p)$ that contains $\mathbb{Z}_p$;*
- *n be a natural number such that $n \mid p-1$;*
- *K be an H-invariant subgroup of $(\mathbb{Z}_n)^p$; and*
- *$\phi \colon H \to (\mathbb{Z}_n)^p/K$ be a crossed homomorphism.*

Then ϕ is cohomologous to a homomorphism from H to $C_0/(K \cap C_0)$, where C_0 is the repetition code in $(\mathbb{Z}_n)^p$.

Remark 2.16 *The conclusion of the theorem can be stated more concretely: If ϕ is not cohomologous to 0, then either*

1. *$H \leq \mathrm{AGL}(1,p)$, and there is some $c \in \mathbb{Z}_n$, and some generator h of $H/\mathbb{Z}_p$, such that $|h|(c, c, \ldots, c) \in K$ and, after replacing ϕ by a cohomologous cocycle, we have $\phi(h^a, z) = a(c, c, \ldots, c)$, for $a \in \mathbb{Z}$ and $z \in \mathbb{Z}_p$; or*
2. *$H = S_p$, n is even, and there is some $c \in \mathbb{Z}_n$, such that $(2c, 2c, \ldots, 2c) \in K$ and, after replacing ϕ by a cohomologous cocycle, we have $\phi(h) = 0 + K$ if $g \in A_p$ or $\phi(h) = (c, c, \ldots, c) + K$ if $g \notin A_p$.*

We now turn to combinatorial topics.

Definition 2.17 A *k-ary relational structure* is an ordered pair (V, E), with V a set and E a subset of V^k. A 3-ary relational structure will be called a *ternary relational structure.*

Definition 2.18 For a group G, define $g_L : G \to G$ by $g_L(h) = gh$, and let $G_L = \{g_L : g \in G\}$. It is easy to verify that G_L is a group, called the *left regular representation of* G. We will say a k-ary relational structure X is a *k-ary Cayley object of* G if $G_L \leq \mathrm{Aut}(X)$ (note that this implies $V = G$). In general, a combinatorial object X will be a *Cayley object of* G if $G_L \leq \mathrm{Aut}(X)$.

Definition 2.19 Let $G \leq S_\Omega$, and $X_1, \ldots, X_r$ be all k-ary relational structures with $G \leq \mathrm{Aut}(X)$. We define the *k-closure of* G, denoted by $G^{(k)}$, to be $\cap_{i=1}^{r} \mathrm{Aut}(X_i)$, and say that G is *k-closed* if $G^{(k)} = G$.

We shall have need of the following results.

Lemma 2.20 ([12]) *For permutation groups $G \leq S_X$ and $H \leq S_Y$, the following hold for every $k \geq 2$:*

1. *Let $G \times H$ act canonically on $X \times Y$. Then $(G \times H)^{(2)} = G^{(k)} \times H^{(k)}$,*
2. *Let $G \wr H$ act canonically on $X \times Y$. Then $(G \wr H)^{(k)} = G^{(k)} \wr H^{(k)}$.*

Lemma 2.21 (Theorem 5.12, [19]) *Let G be a permutation group acting on Ω. Let $k \geq 2$ and suppose there exists $\alpha_1, \ldots, \alpha_{k-1} \in \Omega$ such that $G_{\alpha_1 \ldots \alpha_{k-1}} = 1$ ($G_{\alpha_1 \ldots \alpha_{k-1}}$ is the stabilizer of the points $\alpha_1, \ldots, \alpha_{k-1}$). Then $G^{(k)} = G$.*

3 Results

We begin by determining the orders of Sylow p-subgroups in k-closed groups of degree p^2. We have the following preliminary result.

Lemma 3.1 *Let X be a vertex-transitive k-ary relational structure of order p^2 such that $k \leq p$ and $G \leq \mathrm{Aut}(X)$ such that G is a transitive subgroup of $\mathrm{Aut}(X)$ that admits a complete block system $\mathcal{B}$ of p blocks of size p. Suppose that whenever $B_1, \ldots, B_{k-1}, B_k$ are distinct blocks of $\mathcal{B}$, then there exists $\gamma \in \mathrm{fix}_G(\mathcal{B})$ such that $\gamma|_{B_i} = 1$, $1 \leq i \leq k-1$, and $\gamma|_{B_k} \neq 1$. Then a Sylow p-subgroup of $\mathrm{Aut}(X)$ is isomorphic to $\mathbb{Z}_p \wr \mathbb{Z}_p$.*

PROOF. Let P be a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$. Then P is nontrivial, and so $P|_B$ is a cyclic group of order and degree p for every $B \in \mathcal{B}$. For $B \in \mathcal{B}$, define $z_B : V(X) \to V(X)$ by $z_B(x) = x$ if $x \notin B$ and $z_B(x) = \delta_B(x)$, where $\delta_B \in P$ and $\langle (\delta_B)|_B \rangle = P|_B$. We will show that $z_B \in \mathrm{Aut}(X)$ for every $B \in \mathcal{B}$. As $P|_B = \langle z_B \rangle$ for every $B \in \mathcal{B}$, we will then have that $|P| = p^p$

so that a Sylow p-subgroup of $\mathrm{Aut}(X)$ has order p^{p+1}. Thus a Sylow p-subgroup of $\mathrm{Aut}(X)$ is a Sylow p-subgroup of S_{p^2}, which is isomorphic to $\mathbb{Z}_p \wr \mathbb{Z}_p$.

Let $e = (x_1, \ldots, x_k) \in E(X)$, and $B_1, \ldots, B_j$ be the blocks of $\mathcal{B}$ such that for each x_i, $1 \leq i \leq k$, there exists B_ℓ, $1 \leq \ell \leq j$ such that $x_i \in B_\ell$ and if $1 \leq \ell \leq j$, then there exists $1 \leq i \leq k$ such that $x_i \in B_\ell$. That is, $B_1, \ldots, B_j$ is the shortest list of distinct blocks of $\mathcal{B}$ such that $x_i \in \cup_{\ell=1}^{j} B_\ell$, $1 \leq i \leq k$. Clearly $j \leq k$. By hypothesis, for $1 \leq \ell \leq j$ there exists $\gamma_\ell \in \mathrm{fix}_G(\mathcal{B})$ such that $\gamma_\ell|_{B_\ell} \neq 1$ but $\gamma_\ell|_{B_i} = 1$ for every $i \neq \ell$, $1 \leq i \leq j$. Let H_ℓ denote the normal closure of $\langle \gamma_\ell \rangle$ in $\mathrm{fix}_G(\mathcal{B})$. Then of course, $H_\ell \lhd \mathrm{fix}_G(\mathcal{B})$ so that $H_\ell|_B \lhd \mathrm{fix}_G(\mathcal{B})|_B$ for every $B \in \mathcal{B}$. Furthermore, $H_\ell|_{B_i} = 1$ for every $1 \leq i \leq j$, $i \neq \ell$, and as a normal subgroup of a primitive group is transitive [17, Theorem 8.8] and a transitive group of prime degree is primitive [17, Theorem 8.3], we have that $H_\ell|_{B_\ell}$ is transitive. Whence $H_\ell|_{B_\ell}$ contains a p-cycle. We may thus assume without loss of generality that $\gamma_\ell|_{B_\ell}$ is a p-cycle, $1 \leq \ell \leq j$. Raising each γ_ℓ to an appropriate power, we may also assume that each γ_ℓ has order p. By conjugating each γ_ℓ by an appropriate element of $\mathrm{fix}_G(\mathcal{B})$, we may additionally assume that $\gamma_\ell \in P$, $1 \leq \ell \leq j$. Note that for each $1 \leq \ell \leq j$, there exists $a_\ell \in \mathbb{Z}_p$ such that $\gamma_\ell^{a_\ell}|_{B_\ell} = z_{B_\ell}$. Thus by raising each γ_ℓ, $1 \leq \ell \leq j$, to an appropriate power, we assume that $\gamma_\ell|_{B_\ell} = z_{B_\ell}$. Clearly, if $B \neq B_\ell$ for any $1 \leq \ell \leq j$, then $z_B(e) = e$. If $B = B_\ell$ for some $1 \leq \ell \leq j$, then $\gamma_\ell(e) = z_{B_\ell}(e)$, so that $z_{B_\ell}(e) \in E(X)$. We conclude that $z_B \in \mathrm{Aut}(X)$ for every $B \in \mathcal{B}$, and the result follows.

□

Lemma 3.2 *Let P be a transitive p-subgroup of S_{p^2} that is not isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. Then P is contained in a unique Sylow p-subgroup of S_{p^2}.*

PROOF. If P is a Sylow p-subgroup of S_{p^2}, then the result is trivial. Otherwise, $|P| \leq p^p$. By the comment following Theorem 2.8, we may assume without loss of generality that either $(\mathbb{Z}_{p^2})_L \leq P$ or $(\mathbb{Z}_p^2)_L \leq P$. Suppose that P is contained in Sylow p-subgroups Π_1 and Π_2 of S_{p^2}. Then there exists $\delta \in S_{p^2}$ such that $\delta^{-1}\Pi_2\delta = \Pi_1$. Whence $\delta^{-1}P\delta \leq \Pi_1$ and $P \leq \Pi_1$.

By [17, Exercise 6.5], a regular cyclic subgroup admits a unique complete block system of p blocks of size p. As $\mathbb{Z}_p \wr \mathbb{Z}_p$ contains a regular cyclic subgroup, $\mathbb{Z}_p \wr \mathbb{Z}_p$ admits a unique complete block system $\mathcal{B}$ consisting of p blocks of size p. Now, if $|P| \geq p^3$, then by [8, Theorem 14], $P^{(2)} = \mathbb{Z}_p \wr \mathbb{Z}_p$. By [18, Theorem 4.11], the blocks of P are the same as the blocks of $P^{(2)}$, and so P admits $\mathcal{B}$ as a unique complete block system of p blocks of size p. The only remaining possibility for P is that it is a regular subgroup, and if P is cyclic, then by the reference above P admits $\mathcal{B}$ as a unique complete block system. Otherwise, $P \cong \mathbb{Z}_p^2$, so in every case P admits $\mathcal{B}$ as a unique complete block system.

As $\mathcal{B}$ is a block system of $\mathbb{Z}_p \wr \mathbb{Z}_p \geq \delta^{-1}P\delta$, $\mathcal{B}$ is a block system of $\delta^{-1}P\delta$. Clearly then $P/\mathcal{B} = \delta^{-1}P\delta/\mathcal{B} \cong \mathbb{Z}_p$. Furthermore, as there is a unique cyclic code of length p over $GF(p)$ of a given dimension, the code of P induced by $\mathcal{B}$ must be the same as the code of $\delta^{-1}P\delta$ induced by $\mathcal{B}$, so that $\mathrm{fix}_P(\mathcal{B}) = \mathrm{fix}_{\delta^{-1}P\delta}(\mathcal{B})$ and $P = \delta^{-1}P\delta$. Then $\delta \in N_{S_{p^2}}(P)$ and all such elements normalize Π_1 by [8, Lemmas 5 and 6]. Whence $\Pi_1 = \Pi_2$.
□

Lemma 3.3 *Let P be a transitive p-subgroup of S_{p^2} admitting a complete block system $\mathcal{B}$ of p blocks of size p. If $|P| \geq p^{k+1}$, then a Sylow p-subgroup of $P^{(k)}$ is isomorphic to $\mathbb{Z}_p \wr \mathbb{Z}_p$, $k \geq 2$.*

PROOF. Let X be a k-ary relational structure such that $P \leq \mathrm{Aut}(X)$. We will show that a Sylow p-subgroup of $\mathrm{Aut}(X)$ is isomorphic to $\mathbb{Z}_p \wr \mathbb{Z}_p$. As P is contained in a unique Sylow p-subgroup of S_{p^2} by Lemma 3.2, the result will follow. In order to apply Lemma 3.1, we will show that whenever $B_1, \ldots, B_{k-1}, B_k$ are distinct blocks of $\mathcal{B}$, then there exists $\gamma \in \mathrm{fix}_P(\mathcal{B})$ such that $\gamma|_{B_i} = 1$, $1 \leq i \leq k-1$, and $\gamma|_{B_k} \neq 1$. By Lemma 2.4, the code C_P induced by P is a cyclic code of length p over $GF(p)$. We remark that it suffices to show that C_P contains a codeword that is 0 in any fixed $k-1$ coordinates, and non-zero in every other. Note that C_P contains a cyclic code C of dimension k. By [3, Lemma, pg. 127], C is maximal distance separable so that the minimum distance in C is exactly $p-k+1$. By [14, Theorem 11.4], C has a minimum weight codeword in any $p-k+1$ coordinates. The result then follows. □

Corollary 3.4 *Let X be a k-ary relational structure of order p^2, with Sylow p-subgroup P. Then P is k-closed and*

- *if P contains a regular cyclic subgroup, then P is conjugate to one of $P_1, \ldots, P_{k-1}$, or $\mathbb{Z}_p \wr \mathbb{Z}_p$, or*
- *if P contains a regular elementary abelian subgroup, then P is conjugate to one of $P_1', \ldots, P_{k-1}'$, or $\mathbb{Z}_p \wr \mathbb{Z}_p$.*

PROOF. By the comment following Theorem 2.8, we may assume without loss of generality that either $\langle \tau \rangle \leq P$ or $\langle \rho_1, \rho_2 \rangle \leq P$, where τ, ρ_1, and ρ_2 are as in Definition 2.7. Thus $P = P_i$ if $\langle \tau \rangle \leq P$ or $P = P_i'$ if $\langle \rho_1, \rho_2 \rangle \leq P$ by Theorem 2.8, $1 \leq i \leq p$. By Lemma 3.3, either $P = \mathbb{Z}_p \wr \mathbb{Z}_p$ or $|P| \leq p^k$. Thus $P = P_i$ if $\langle \tau \rangle \leq P$ or $P = P_i'$ if $\langle \rho_1, \rho_2 \rangle \leq P$, $1 \leq i \leq k-1$, or $P \cong \mathbb{Z}_p \wr \mathbb{Z}_p$. By [18, Exercise 5.28 and Theorem 5.10], the k-closure of any p-group is a p-group, so that $P \leq P^{(k)} \leq \mathbb{Z}_p \wr \mathbb{Z}_p$ (as $\mathbb{Z}_p \wr \mathbb{Z}_p$ is a

Sylow p-subgroup of S_{p^2}). Hence $\mathbb{Z}_p \wr \mathbb{Z}_p$ is k-closed for every $k \geq 2$. It $P \ncong \mathbb{Z}_p \wr \mathbb{Z}_p$, then let $\mathcal{B}$ be a complete block system of P consisting of p blocks of size p, with C_P the code induced by P. Let C_P have dimension i, so that $1 \leq i \leq k-1$. By [3, Lemma, pg. 127], C_P is maximal distance separable so that the minimum distance in C_P is exactly $p-i+1$. Let c be a codeword of C_P of minimum distance $p-i+1$, with $\gamma \in \mathrm{fix}_P(\mathcal{B})$ such that $v(\gamma) = c$ (v is defined as in Lemma 2.4). Then γ acts trivially on exactly $i-1$ blocks of $\mathcal{B}$, say $B_1, \ldots, B_{i-1}$. Choose $x_j \in B_j$, $1 \leq j \leq i-1$, and x_i to be any point not contained in $\cup_{j=1}^{i} B_i$. Let $\gamma' \in G_{x_1 \ldots x_i}$. Then $\gamma \in \mathrm{fix}_P(\mathcal{B})$ and the weight of $v(\gamma')$ is less than that of γ, and so $\gamma' = 1$. Then P is k-closed by Lemma 2.21. □

The following results follow directly from Lemma 3.3, Corollaries 1 and 2 of [8], and the results implicit in [9] and [2] regarding conjugates of regular subgroups of groups that contain a full Sylow p-subgroup of S_{p^2}. In order to succinctly state these results, we will need some notation. Let $\beta \in \mathbb{Z}_p^*$ be of order $p-1$. Define $\bar{\beta}, \tilde{\beta} : \mathbb{Z}_p^2 \to \mathbb{Z}_p^2$ by $\bar{\beta}(i,j) = (\beta i, j)$ and $\tilde{\beta}(i,j) = (i, \beta j)$. For $\omega \in \mathbb{Z}_{p^2}^*$ of order $p-1$, define $\hat{\omega} : \mathbb{Z}_{p^2} \to \mathbb{Z}_{p^2}$ by $\hat{\omega}(i) = \omega i$.

Corollary 3.5 *Let X and Y be Cayley k-ary relational structures of $\mathbb{Z}_{p^2}$, $k \leq p$, such that a Sylow p-subgroup of $\mathrm{Aut}(X)$ has order p^{i+1}, for some $1 \leq i \leq p$. Then $i = 1, 2, \ldots, k-1$, or p and*

1. *if $i = 1, \ldots, k-1$, then X and Y are isomorphic if and only if they are isomorphic by $\alpha = \hat{\omega}^j \gamma_{i+1}^{\ell}$, for some $1 \leq j \leq p-1$ and $0 \leq \ell \leq p-1$,*
2. *if $i = p$, then X and Y are both canonically Cayley k-ary relational structures of $\mathbb{Z}_p^2$, and are isomorphic if and only if they are isomorphic by $\bar{\beta}^j \tilde{\beta}^{\ell}$, for some $1 \leq j, \ell \leq p-1$.*

Corollary 3.6 *Let X and Y be Cayley objects of $\mathbb{Z}_p^2$ with Π_1 a Sylow p-subgroup of $\mathrm{Aut}(X)$ and Π_2 a Sylow p-subgroup of Y. Let $\alpha_1 \in \mathrm{Aut}(\mathbb{Z}_p^2)$ such that $\alpha_1 \Pi_1 \alpha_1^{-1} = P_i'$ and $\alpha_2 \in \mathrm{Aut}(\mathbb{Z}_p^2)$ such that $\alpha_2 \Pi_2 \alpha_2^{-1} = P_i'$, $1 \leq i \leq p$. Then $i = 1, \ldots, k-1$ or p and*

1. *if $i = 1, \ldots, k-1$, then X and Y are isomorphic if and only if they are isomorphic by $\alpha_2^{-1} \bar{\beta}^j \tilde{\beta}^k \gamma_{i+1}^{\ell} \alpha_1$, $1 \leq j, k \leq p-1$, $0 \leq \ell \leq p-1$,*
2. *if $i = p$, then X and Y are isomorphic if and only if they are isomorphic by a group automorphism of $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Lemma 3.7 *Let $G \leq S_{p^2}$ be transitive such that G admits a complete block system $\mathcal{B}$ of p blocks of size p and a Sylow p-subgroup P of G has order at least p^4. Then $\mathrm{fix}_{G^{(3)}}(\mathcal{B}) = 1_{S_p} \wr (\mathrm{fix}_{G^{(3)}}(\mathcal{B})|_B)$.*

PROOF. As $|P| \geq p^4$, it follows by Lemma 3.3 that P is isomorphic to $\mathbb{Z}_p \wr \mathbb{Z}_p$. Let $\rho \in \mathrm{fix}_P(\mathcal{B})$ such that ρ is semiregular of order p. Then $\rho|_B \in G^{(3)}$ for every $B \in \mathcal{B}$. Let $e = (x_1, x_2, x_3) \in E(X)$, where X is a ternary relational structure with $G \leq \mathrm{Aut}(X)$. We will show that if $\gamma \in \mathrm{fix}_{G^{(3)}}(\mathcal{B})$, then $(\gamma|_B)(e) \in E(X)$. If there exists $B' \in \mathcal{B}$ such that $x_1, x_2, x_3 \in B'$, then clearly $(\gamma|_B)(e) \in E(X)$ for every $\gamma \in \mathrm{fix}_{G^{(3)}}(\mathcal{B})$ as $(\gamma|_B)(e) = e$ or $(\gamma|_B)(e) = \gamma(e)$. If there exist distinct blocks $B_1, B_2, B_3 \in \mathcal{B}$ such that $x_1 \in B_1$, $x_2 \in B_2$, and $x_3 \in B_3$, then, as noted above, $\rho|_{B_i} \in G^{(3)}$ for $1 \leq i \leq 3$. Applying $\rho|_{B_1}$ to e $p-1$ times, we have that $(x_1', x_2, x_3) \in E(X)$ for every $x_1' \in B_1$. Applying $\rho|_{B_2}$ to each of the p edges (x_1', x_2, x_3), $x_1' \in B_1$, $p-1$ times gives that $(x_1', x_2', x_3) \in E(X)$ for every $x_1' \in B_1$ and $x_2' \in B_2$. Finally, applying $\rho|_{B_3}$ to each of the p^2 edges (x_1', x_2', x_3), $x_1' \in B_1$, $x_2' \in B_2$, $p-1$ times yields that $(x_1', x_2', x_3') \in E(X)$ for every $x_1' \in B_1$, $x_2' \in B_2$, and $x_3' \in B_3$. Then $\gamma(e) \in E(X)$ for every $\gamma \in 1_{S_p} \wr S_p$ so clearly $(\gamma|_B)(e) \in E(X)$ for every $B \in \mathcal{B}$. If there exist distinct blocks $B_1, B_2 \in \mathcal{B}$ such that $x_1, x_2 \in B_1$ and $x_3 \in B_2$, then applying $\rho|_{B_2}$ to e $p-1$ times gives that $(x_1, x_2, x_3') \in E(X)$ for every $x_3' \in B_2$. Clearly if $B \neq B_1, B_2$, then $(\gamma|_B)(e) = e$ for every $\gamma \in \mathrm{fix}_{G^{(3)}}(B)$. If $\gamma \in \mathrm{fix}_{G^{(3)}}(\mathcal{B})$, then $\gamma(e) = (\gamma(x_1), \gamma(x_2), \gamma(x_3))$. Applying $\rho|_{B_2}$ to $(\gamma(x_1), \gamma(x_2), \gamma(x_3))$ $p-1$ times, we have that $(\gamma(x_1), \gamma(x_2), x_3') \in E(X)$ for every $x_3' \in B_2$. Then $(\gamma(x_1), \gamma(x_2), x_3) = (\gamma|_{B_1})(e) \in E(X)$. Finally, $(\gamma|_{B_2})(e) = (x_1, x_2, \gamma(x_3))$. As $(x_1, x_2, x_3') \in E(X)$ for every $x_3' \in B_2$, $(\gamma|_{B_2})(e) \in E(X)$. Whence $\gamma|_B \in G^{(3)}$ for every $B \in \mathcal{B}$ and $\gamma|_B \in \mathrm{fix}_{G^{(3)}}(\mathcal{B})$ as required. □

Lemma 3.8 *Let $p \geq 5$ and $G \leq S_{p^2}$ be transitive such that G admits a complete block system $\mathcal{B}$ of p blocks of size p and a Sylow p-subgroup P of G has order at least p^4. If $\mathrm{fix}_{G^{(3)}}(\mathcal{B})|_B = A_p$ or S_p, then $G^{(3)} = (G/\mathcal{B})^{(3)} \wr S_p$.*

PROOF. As $p \geq 5$, $\mathrm{fix}_{G^{(3)}}(\mathcal{B})|_B \geq A_p$ is a doubly transitive group with nonabelian socle for every $B \in \mathcal{B}$. Let K_B be the normal closure of $\langle \rho|_B \rangle$ in $\mathrm{fix}_{G^{(3)}}(\mathcal{B})|_B$, where $\rho \in \mathrm{fix}_G(\mathcal{B})$ is any semiregular element of order p. As $K_B \trianglelefteq \mathrm{fix}_{G^{(3)}}(\mathcal{B})|_B$, $K_B \cong A_p$ or S_p for every $B \in \mathcal{B}$. We conclude that $G^{(3)}$ contains a transitive subgroup isomorphic to $\mathbb{Z}_p \wr A_p$ by Lemma 3.7, and hence by Lemma 2.20, we have that $(\mathbb{Z}_p \wr A_p)^{(3)} = (\mathbb{Z}_p)^{(3)} \wr (A_p)^{(3)} \leq G^{(3)}$. As $\mathbb{Z}_p$ is regular, by Theorem 2.21 $(\mathbb{Z}_p)^{(2)} = \mathbb{Z}_p$, and so $(\mathbb{Z}_p)^{(3)} = (\mathbb{Z}_p)^{(2)(3)} = \mathbb{Z}_p$ by [18, Theorem 5.10]. As $3 \leq p-2$ and A_p is $(p-2)$-transitive, we have that $A_p^{(3)} = S_p$. Thus $\mathbb{Z}_p \wr S_p \leq G^{(3)}$ and $\mathrm{fix}_{G^{(3)}}(\mathcal{B}) = 1_{S_p} \wr S_p$. By [15, Theorem 2.6] we have that $G^{(3)} = (G^{(3)}/\mathcal{B}) \wr S_p$. Note that $(G/\mathcal{B}) \wr S_p \leq G^{(3)}$ so by Lemma 2.20, $(G/\mathcal{B})^{(3)} \wr S_p \leq G^{(3)}$. As $G^{(3)}/\mathcal{B} \leq (G/\mathcal{B})^{(3)}$, the result follows.

□

We will now calculate the full automorphism groups of ternary relational structures of some prime-squared orders. Again, we begin with a preliminary result. For p a prime, let $M(p) = \{x \to ax : a \in \mathbb{Z}_p^*\}$.

Lemma 3.9 *Let p be a prime such that the only doubly transitive non-abelian simple group of degree p is A_p. Let $G \leq S_{p^2}$ be transitive such that G is imprimitive with Sylow p-subgroup of order at least p^4. Then one of the following is true for some $A, B \leq \mathrm{AGL}(1,p)$:*

1. $G^{(3)} = S_p \wr S_p$,
2. $G^{(3)} = A \wr S_p$,
3. $G^{(3)} = S_p \wr A$, *or*
4. $G^{(3)} = G_{B,\mathbb{Z}_p,A^p,\phi}$. *Furthermore, there is some $c \in M(p)$, and some generator h of $B/\mathbb{Z}_p$, such that $(c^{|h|}, c^{|h|}, \ldots, c^{|h|}) \in A^p$ and we have $\phi(h^a, z) = (c^a, c^a, \ldots, c^a)$ for $a \in \mathbb{Z}$ and $z \in \mathbb{Z}_p$.*

PROOF. As G is imprimitive, $G^{(3)}$ admits a complete block system $\mathcal{B}$ of p blocks of size p. Let P be a Sylow p-subgroup of $G^{(3)}$. As $|P| \geq p^4$, it follows by Lemma 3.7 that $\mathrm{fix}_{G^{(3)}}(\mathcal{B}) = 1_{S_p} \wr (\mathrm{fix}_{G^{(3)}}(\mathcal{B})|_B)$.

If $\mathrm{fix}_{G^{(3)}}(\mathcal{B})|_B$ is a doubly transitive group with nonabelian socle for some $B \in \mathcal{B}$, then $\mathrm{fix}_{G^{(3)}}(\mathcal{B})|_B = A_p$ or S_p and by Lemma 3.8, $G^{(3)} = (G/\mathcal{B})^{(3)} \wr S_p$. If $(G/\mathcal{B})^{(3)} \leq \mathrm{AGL}(1,p)$ then (2) follows. Otherwise, by Theorem 2.1, $(G/\mathcal{B})^{(3)}$ is a doubly-transitive group with nonabelian socle, so that $(G/\mathcal{B})^{(3)} = A_p$ or S_p. As S_3 is solvable, $p \geq 5$, so that A_p is $(p-2) \geq 3$ transitive. Hence $(G/\mathcal{B})^{(3)} = S_p$ and (1) follows. We henceforth assume that $\mathrm{fix}_{G^{(3)}}(\mathcal{B})|_B$ is solvable, so that $\mathrm{fix}_{G^{(3)}}(\mathcal{B})|_B = A \leq \mathrm{AGL}(1,p)$ and $\mathrm{fix}_{G^{(3)}}(\mathcal{B}) = A^p$.

By Proposition 2.13, there exists

1. H and L transitive subgroups of S_p such that L is simple;
2. K/L^p an H-invariant subgroup of the abelian group $(N_{S_p}(L)/L)^p$;
3. $\phi\colon H \to N_{S_p}(L)^p/K$ a crossed homomorphism; and
4. $G_{H,L,K,\phi} = \{\, (h,v) \in H \ltimes N_{S_p}(L)^p : \phi(h) = vK \,\} \leq S_p \wr S_p$,

such that $G^{(3)} = G_{H,L,K,\phi}$. As $\mathrm{fix}_{G^{(3)}}(\mathcal{B}) = A^p$, we have that $L = \mathbb{Z}_p$ and $N_{S_p}(L) = \mathrm{AGL}(1,p)$. We now show that if $G^{(3)}/\mathcal{B}$ is a doubly-transitive group with nonabelian socle, then $G^{(3)}/\mathcal{B} = S_p$.

If $G^{(3)}/\mathcal{B}$ is doubly-transitive with nonabelian socle (and so $p \geq 5$ and A_p is 3-transitive), then $G^{(3)}/\mathcal{B} \cong A_p$ or S_p. In either case, there exists $H \leq G^{(3)}$ such that $H/\mathcal{B} = A_p$. As ϕ is cohomologous to 0 (see Theorem

2.15 and the remark following it), we have that $G^{(3)}$ contains a subgroup isomorphic to $A_p \wr \mathbb{Z}_p$ and so $G^{(3)}$ contains a subgroup isomorphic to $A_p \times \mathbb{Z}_p$. By Lemma 2.20, $G^{(3)}$ contains a subgroup isomorphic to $S_p \times \mathbb{Z}_p$. Hence $G^{(3)}/\mathcal{B} = S_p$.

By Theorem 2.1, we then have that $G^{(3)}/\mathcal{B} = S_p$ or $G^{(3)}/\mathcal{B} = B \leq \mathrm{AGL}(1,p)$. Thus $H \leq \mathrm{AGL}(1,p)$ or $H = S_p$. As $\phi(1) = K = \mathrm{fix}_{G^{(3)}}(\mathcal{B})$, we have that $K = A^p$ for some $A \leq \mathrm{AGL}(1,p)$ as above. Note then that $N_{S_p}(L)^p/K \cong (N_{S_p}(L)/\mathbb{Z}_p)^p/(K/\mathbb{Z}_p) \cong C^p$, where $C \leq M(p)$, and $M(p)$ is a cyclic group of order $p-1$. By Theorem 2.15 and the remark following it, either ϕ is cohomologous to 0 or (1) or (2) of Remark 2.16 hold. If ϕ is cohomologous to 0, then clearly $G^{(3)} = S_p \wr A$ or $B \wr A$, where $B \leq \mathrm{AGL}(1,p)$ and either (3) or (4) follow. Otherwise, (1) or (2) of Remark 2.16 holds. Recall that if $G^{(3)}/\mathcal{B} = S_p$ then $S_p \times \mathbb{Z}_p \leq G^{(3)}$. This implies that if $G^{(3)}/\mathcal{B} = S_p$, then ϕ is cohomologous to 0. Hence (2) of Remark 2.16 holds and so (4) follows. □

Theorem 3.10 *Let G be a 3-closed subgroup of S_{p^2} that contains the left regular representation of $\mathbb{Z}_{p^2}$, and the only nonsolvable doubly transitive groups of degree p are A_p or S_p. Then one of the following is true:*

1. *G is doubly transitive and $G = S_{p^2}$, or $\mathrm{PSL}(n,k) \leq G \leq \mathrm{P\Gamma L}(n,k)$, where $(k^n-1)/(k-1) = p^2$,*
2. *G is imprimitive and one of the following is true:*
   (a) *$G \leq N_{S_{p^2}}((\mathbb{Z}_{p^2})_L)$,*
   (b) *$G \leq N_{S_{p^2}}(P_2)$,*
   (c) *$G = G_1 \wr G_2$, where G_1 and G_2 are 3-closed groups of degree p, or*
   (d) *$G = G_{B,\mathbb{Z}_p,A^p,\phi}$, where $A, B \leq \mathrm{AGL}(1,p)$. Furthermore there is some $c \in M(p)$, and some generator h of $B/\mathbb{Z}_p$, such that $(c^{|h|}, c^{|h|}, \ldots, c^{|h|}) \in A^p$ and we have $\phi(h^a, z) = (c^a, c^a, \ldots, c^a)$ for $a \in \mathbb{Z}$ and $z \in \mathbb{Z}_p$.*

PROOF. As $\mathbb{Z}_{p^2}$ is a Burnside group, if $G \leq S_{p^2}$ such that $(\mathbb{Z}_{p^2})_L \leq G$, then G is doubly transitive or imprimitive [17, Theorem 25.3]. If G is doubly transitive, then (1) follows from Theorem 2.10 and the Remark following it. If G is imprimitive, by Lemma 3.3, we have that a Sylow p-subgroup P of G has order p^2, p^3, or p^{p+1}. If $|P| = p^2$, then (2a) follows from Theorem 2.10, while if $|P| = p^3$, (2b) follows from Theorem 2.10 as well. Finally, if $|P| = p^{p+1}$, then (2c) or (2d) follows from Lemma 3.9. □

Theorem 3.11 *Let G be a 3-closed subgroup of S_{p^2} such that G contains the left regular representation of $\mathbb{Z}_p^2$ and the only nonsolvable doubly transitive groups of degree p are A_p and S_p.*

1. *If G is doubly transitive, then $G = S_{p^2}$, or $(\mathbb{Z}_p)_L < G \leq \mathrm{AGL}(2,p)$.*
2. *If G is simply primitive and solvable, then $G \leq \mathrm{AGL}(2,p)$.*
3. *If G is simply primitive and nonsolvable, then $G = S_2 \wr S_p$ in its product action or $G \leq \mathrm{AGL}(2,p)$.*
4. *If G is imprimitive, solvable, and has elementary abelian Sylow p-subgroup, then $G \leq \mathrm{AGL}(1,p) \times \mathrm{AGL}(1,p)$.*
5. *If G is imprimitive, nonsolvable, and has elementary abelian Sylow p-subgroup, then either $G = S_p \times S_p$ or $G = S_p \times A$, where $A \leq \mathrm{AGL}(1,p)$.*
6. *If G is imprimitive and has Sylow p-subgroup P_2' of order p^3, then $G \leq N_{S_{p^2}}(P_2')$.*
7. *If G is imprimitive with Sylow p-subgroup of order at least p^4, then*
   (a) *$G = G_1 \wr G_2$, where G_1 and G_2 are 3-closed groups of degree p, or*
   (b) *$G = G_{H,\mathbb{Z}_p,A^p,\phi}$, $A, H \leq \mathrm{AGL}(1,p)$. Furthermore, there is some $c \in \mathbb{Z}_n$, $n|(p-1)$, and some generator h of $H/\mathbb{Z}_p$, such that $|h|(c,c,\ldots,c) \in K$ and have $\phi(h^a,z) = a(c,c,\ldots,c)$, for $a \in \mathbb{Z}$ and $z \in \mathbb{Z}_p$.*

PROOF. (1) If G is doubly transitive, then by Theorem 2.10 and the remarks following it $G = A_{p^2}$, S_{p^2}, or $(\mathbb{Z}_p^2)_L < G \leq \mathrm{AGL}(2,p)$. If $G = A_{p^2}$ and $p^2 \neq 4$, then G is $p^2 - 2 \geq 7$ transitive. Whence $A_{p^2}^{(3)} = S_{p^2}$. If $p^2 = 4$, then $S_4 = AGL(2,2)$.

(4) and (5) By Theorem 2.10, $G \leq S_p \times S_p$. If G is solvable, then $G \leq \mathrm{AGL}(1,p) \times \mathrm{AGL}(1,p)$. If G is nonsolvable, then $G \leq H \times K$, where $H, K \leq S_p$, and one of H and K are nonsolvable. Thus $p \geq 5$. By Theorem 2.1, if H or K is nonsolvable, then H or K is doubly transitive. As the only nonsolvable doubly transitive groups of degree p are A_p and S_p, A_p or S_p are both at least 3-transitive. It then follows by Theorem 2.20 that $G^{(3)} = H^{(3)} \times K^{(3)} = S_p \times S_p$ or $S_p \times A$, where $A \leq \mathrm{AGL}(1,p)$.

(2) and (3) By Theorem 2.10 either $G \leq \mathrm{AGL}(2,p)$ or G has a transitive, imprimitive subgroup $H \leq S_p \times S_p$ of index 2. We thus assume that G has an imprimitive subgroup $H \leq S_p \times S_p$ of index 2. If G is solvable, then H is solvable so that $H \leq \mathrm{AGL}(1,p) \times \mathrm{AGL}(1,p)$. Whence H has a unique Sylow

p-subgroup $P \cong \mathbb{Z}_p \times \mathbb{Z}_p$ which is characteristic in G. Thus $G \leq \mathrm{AGL}(2,p)$. If G is nonsolvable, then H is nonsolvable. By (4) and (5), $H^{(3)} = S_p \times A$ or $S_p \times S_p$. As $H \lhd G$, $\mathrm{soc}(G)$ is nontrivial. Furthermore, as H is nonsolvable and $H \leq S_p \times S_p$, $\mathrm{soc}(G) \ncong \mathbb{Z}_p \times \mathbb{Z}_p$. We conclude that the socle type of G is A_p. By the O'Nan-Scott Theorem [7, Theorem 4.6A], $\mathrm{soc}(G) \cong A_p$, $\mathrm{soc}(G) \cong A_p^3$, and G is of diagonal type, or $\mathrm{soc}(G) \cong A_p^2$, and G is a subgroup of $S_2 \wr U$ in its product action, where U is a primitive nonregular group. As G is primitive and $\mathrm{soc}(G) \lhd G$, if $\mathrm{soc}(G) = A_p$, then $\mathrm{soc}(G)$ is not transitive and so the orbits of $\mathrm{soc}(G)$ form a nontrivial complete block system of G. This contradicts the assumption that G is primitive. As $\mathrm{soc}(G) \leq H$, $|\mathrm{soc}(G)| \leq |A_p|^2$ so that $\mathrm{soc}(G) \ncong A_p^3$. Whence $\mathrm{soc}(G) \cong A_p^2$ and G is a subgroup of $S_2 \wr U$ in its product action, where U is a primitive nonregular group. As $\mathrm{soc}(G) = A_p^2$, $H^{(3)} = S_p \times S_p$ so that $U = S_p$ as required.

(6) This follows directly from Theorem 2.10.

(7) This follows directly from Lemma 3.9. □

We remark that neither of the two preceding results claim that *all* of the groups given are 3-closed, just that all 3-closed groups of the appropriate degree occur on the appropriate lists.

Finally, we would like to point out that the above results have implications for more general combinatorial structures. We define a *relational structure* X to be an ordered pair $(V(X), E(X))$, where $V(X)$ is a set and $E(X)$ is a subset of $\cup_{i=1}^{k}(V(X)^i)$, for some $k \in \mathbb{Z}^+$. If $e \in E(X)$, then $e = (x_1, \ldots, x_\ell)$ for some $\ell \in \mathbb{Z}^+$. We define the *length of* e to be ℓ. We remark that every hypergraph is a relational structure.

Proposition 3.12 *Let X be a relational structure such that X has maximum edge length k. Then* $\mathrm{Aut}(X)$ *is k-closed.*

PROOF. Let X be a relational structure. Let E_i, $1 \leq i \leq k$ be the set of all edges of X of length i. Let $\alpha \in \mathrm{Aut}(X)$. Clearly $\alpha(E_i) = E_i$ for every $1 \leq i \leq k$. Define i-ary relational structures X_i, $1 \leq i \leq k$, by $V(X_i) = V(X)$ and $E(X_i) = E_i$. Clearly if $\alpha \in \mathrm{Aut}(X)$, then $\alpha \in \mathrm{Aut}(X_i)$, $1 \leq i \leq k$. Conversely, if $\alpha \in \mathrm{Aut}(X_i)$, $1 \leq i \leq k$, then $\alpha(E_i) = E_i$ for every $1 \leq i \leq k$ and so $\alpha(e) \in E(X)$ for every $e \in E(X)$. Thus $\mathrm{Aut}(X) = \cap_{i=1}^{k}\mathrm{Aut}(X_i)$. As each X_i is an i-ary relational structure, $\mathrm{Aut}(X_i)$ is i-closed for every $1 \leq i \leq k$. It is straightforward to show that the intersection of k-closed groups is k-closed, and by [18, Theorem 5.10], if $\ell \leq k$, then for any group G, $G^{(k)(\ell)} = G^{(\ell)(k)} = G^{\ell}$. As $\mathrm{Aut}(X_i)$ is i-closed, we then have that $\mathrm{Aut}(X_i)$ is k-closed, and as $\mathrm{Aut}(X) = \cap_{i=1}^{k}\mathrm{Aut}(X_i)$, we have that $\mathrm{Aut}(X)$ is k-closed. □

References

[1] Ádám, A., Research problem 2-10, *J. Comb. Theory* **2** (1967), 393.

[2] Alspach, B., and Parsons, T. D., Isomorphism of circulant graphs and digraphs, *Discrete Math.* 25 (1979), no. 2, 97–108.

[3] Assmus, E. F., and Mattson, H. F., New 5-designs, *J. Combin. Theory* **6** (1969), 122–151.

[4] Burnside, W., On some properties of groups of odd order, *J. London Math. Soc.* 33 (1901) 162–185.

[5] Cameron, P.J., Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* 13 (1981) 1–22.

[6] Cartan, H., and Eilenberg, S., *Homological Algebra,* Princeton University Press, Princeton, 1956.

[7] Dixon, J.D., and Mortimer, B., *Permutation Groups*, Springer-Verlag New York, Berlin, Heidelberg, Graduate Texts in Mathematics, **163**, 1996.

[8] Dobson, E., and Witte, D., Transitive permutation groups of prime-squared degree, *J. Algebraic Combin.*, 16 (2002) 43-69.

[9] Godsil, C. D., On Cayley graph isomorphisms, *Ars Combin.* **15** 1983, 231-246.

[10] Huffman, W. C., The equivalence of two cyclic objects on pq elements, *Discrete Math.* 154 (1996) 103–127.

[11] Huffman, W.C., Job, V., and Pless, V., Multipliers and generalized multipliers of cyclic objects and cyclic codes, *J. Combin. Theory Ser. A* 62 (1993) 183–215.

[12] Kalužnin, L. A., and Klin, M. H., On some numerical invariants of permutation groups (in Russian), *Latviĭsk. Mat. Ežegodnik* **18**, 1976, 81-99.

[13] Li, C. H., On isomorphisms of finite Cayley graphs - a survey, *Disc. Math.*, **246** (2002), 301-334.

[14] MacWilliams, F. J., and Sloane, M. J.A., *The Theory of Error Correcting Codes*, North-Holland, New York, 1977.

[15] Meldrum, J. D. P., *Wreath Products of Groups and Semigroups*, Pitman Monographs and Surveys in Pure and Applied Mathematics, **74**, Longman, Harlow, 1995.

[16] Pálfy, P. P., Isomorphism problem for relational structures with a cyclic automorphism, *Europ. J. Comb.* **8** 1987, 35-43.

[17] Wielandt, H. (trans. by R. Bercov), *Finite Permutation Groups*, Academic Press, New York, 1964.

[18] Wielandt, H., Permutation groups through invariant relations and invariant functions, lectures given at The Ohio State University, Columbus, Ohio, 1969.

[19] Wielandt, H., Mathematische Werke/Mathematical works. Vol. 1. Group theory, Walter de Gruyter & Co., Berlin, 1994.