The isomorphism problem for Cayley digraphs on groups of prime-squared order

Anne Joseph*

Department of Mathematics, Williams College, Williamstown, MA 01267, USA

Received 22 May 1992; revised 2 August 1993

Abstract

Given any prime $p$, there are two non-isomorphic groups of order $p^2$. We determine precisely when a Cayley digraph on one of these groups is isomorphic to a Cayley digraph on the other group. Namely, let $X = \text{Cay}(G : T)$ be a Cayley digraph on a group $G$ of order $p^2$ with generating set $T$. We prove that $X$ is isomorphic to a Cayley digraph on both $Z_{p^2}$ and $Z_p \times Z_p$ if and only if $X$ is a lexicographic product of two Cayley digraphs of order $p$. Equivalently, there exists a subgroup $H$ of $G$ of order $p$ such that for every $t \in T \setminus H$, we have $tH \subseteq T$.

1. Introduction

This paper studies the isomorphism problem for Cayley graphs of prime-squared order. We begin with basic definitions before proceeding to the statement of the main result.

Definition. Let $T$ be a subset of a group $G$. The Cayley digraph $\text{Cay}(G : T)$ on $G$ with generating set $T$ is the digraph whose vertex set and edge set are given as follows. The vertex set $V(\text{Cay}(G : T))$ is $G$. The edge set $E(\text{Cay}(G : T))$ is the set of directed edges $[a, b]$ such that $a^{-1}b$ is contained in $T$.

Definition. A Cayley graph is a Cayley digraph $\text{Cay}(G : T)$ such that if $t$ is in $T$ then $t^{-1}$ is also in $T$.

For a basic reference on Cayley graphs, see Biggs [3, pp. 106–107]. Unlike Biggs, we do not assume Cayley digraphs are connected. We do not allow loops or multiple edges in our digraphs.

* Present Address: 4897 Oakcrest Drive, Fairfax, VA 22030, USA.
Definition. We let $\mathbb{Z}_n$ denote the cyclic group of integers modulo $n$.


Given any prime $p$, there are two groups of order $p^2$. We determine precisely when a Cayley digraph on one of these groups is isomorphic to a Cayley digraph on the other group. The following result is proved.

Main Theorem. Let $X = \text{Cay}(G; T)$ be a Cayley digraph on a group $G$ of order $p^2$, where $p$ is prime. Then the following are equivalent:

1. The digraph $X$ is isomorphic to a Cayley digraph on both $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.
2. There exists a subgroup $H$ of $G$ of order $p$ such that for every $t \in T \setminus H$, we have $tH \subseteq T$.
3. There exist Cayley digraphs $U$ and $V$ on $\mathbb{Z}_p$ such that $X$ is isomorphic to the lexicographic product of $U$ and $V$.

Example. The Cayley graph $\text{Cay}(\mathbb{Z}_9; \{1, 3, 6, 8\})$ is not isomorphic to a Cayley graph on $\mathbb{Z}_3 \times \mathbb{Z}_3$. To see this, observe that $H = \langle 3 \rangle$ is the only subgroup of order 3 of $\mathbb{Z}_9$. We have $1 \in \{1, 8\} = T \setminus H$, but $1 + H = \{1, 4, 7\} \not\subseteq T$. Thus, there is some $t \in T \setminus H$ such that we do not have $tH \subseteq T$.

Example. The Cayley graph

\[ \text{Cay}(\mathbb{Z}_3 \times \mathbb{Z}_3; \{(0, 1), (0, 2), (1, 0), (2, 0)\}) \]

is not isomorphic to a Cayley graph on $\mathbb{Z}_9$. To see this, observe that there are four subgroups of order 3 of $\mathbb{Z}_3 \times \mathbb{Z}_3$ and check that for all subgroups $H$, there is some $t \in T \setminus H$ such that we do not have $tH \subseteq T$.

Example. The Cayley digraph $\text{Cay}(\mathbb{Z}_9; \{1, 4, 7\})$ is isomorphic to the Cayley digraph

\[ \text{Cay}(\mathbb{Z}_3 \times \mathbb{Z}_3; \{(1, 0), (1, 1), (1, 2)\}) \]

Let $H = \langle 3 \rangle$. In the first Cayley digraph, for every $t \in T \setminus H = \{1, 4, 7\}$, we have $tH = t + \langle 3 \rangle = T$. In the second Cayley digraph, let $H = \langle (0, 1) \rangle$. For every $t \in T \setminus H = \{(1, 0), (1, 1), (1, 2)\}$, we have $tH = T$. An isomorphism is given by $\varphi(u, v) = u + 3v$ for $0 \leq u, v \leq 3$. 

2. Preliminaries

We present here fundamental concepts from group theory and graph theory that will be utilized in the proof of the Main Theorem. Unless defined otherwise, our notation is consistent with Rotman [8] for group theory and Biggs [3] for graph theory.

Definition. Let $X$ be a graph and $I$ be a subset of $V(X)$. The induced subgraph $X[I]$ is the subgraph of $X$ with $V(X[I]) = I$ and

$$E(X[I]) = \{ [x, y] | [x, y] \in E(X) \text{ and } x, y \in I \}.$$ 

Definition (Sabidussi [10]). Let $X$ and $Y$ be graphs. The lexicographic product $X \text{ lex } Y$ is the graph given as follows: The vertex set $V(X \text{ lex } Y)$ is $V(X) \times V(Y)$. The edge set $E(X \text{ lex } Y)$ is

$$\{ [(x, y), (x', y')] | ([x, x'] \in E(X)) \text{ or } (x = x' \text{ and } [y, y'] \in E(Y)) \}.$$ 

Definition (Rotman [8, p. 184]). The action of a group $G$ on a set $X$ is regular if for every $a, b \in V(X)$, there exists a unique $g \in G$ such that $ga = b$.

The following theorem gives a characterization of Cayley graphs in terms of their automorphism groups. The result is fundamental to our approach to the Cayley digraph isomorphism problem. The cited references prove this result for graphs. Only minor changes to the proof are needed to prove the same result for digraphs.

Theorem 2.1 (Sabidussi [9] or [3, Lemma 16.3, p. 108]). Let $X$ be a digraph and $G$ be a group. The automorphism group $\text{Aut}(X)$ has a subgroup isomorphic to $G$ that acts regularly on $V(X)$ if and only if $X$ is isomorphic to a Cayley digraph $\text{Cay}(G : T)$ for some subset $T$ of $G$.

The following fact used in the proof of Theorem 2.1 is easy to verify.

Corollary 2.2. If $X = \text{Cay}(G : T)$, then the left regular representation of $G$ is a regular subgroup of $\text{Aut}(X)$.

Definition (Rotman [8, p. 51]). If a group $G$ acts on a set $X$ and $x \in X$, then the stabilizer of $x$, denoted by $\text{Stab}_G(x)$, is the subgroup

$$\text{Stab}_G(x) = \{ g \in G | gx = x \}.$$ 

Lemma 2.3 (Rotman [8, Theorem 3.22, p. 51]). Let a group $G$ act on a set $X$. Then the number of elements in the orbit of $x \in X$ is $[G : \text{Stab}_G(x)]$. 

Lemma 2.4 (Rotman [8, Theorem 9.4, p. 182]). Let a group $G$ act on a set $X$ and let $a, b \in X$. If $b = ga$ for some $g \in G$, then $g\text{Stab}_G(a)g^{-1} = \text{Stab}_G(b)$. In particular, if the action of $G$ is transitive, then all stabilizers are conjugate and have the same order.

Definition (Biggs [3, p. 147]). A $G$-block for the action of a group $G$ on a set $X$ is a proper subset $B$ that contains more than one element of $X$ and satisfies the condition that $B$ and $gB$ are either disjoint or identical, for each $g$ in $G$.

Some authors, such as Hall [5], refer to blocks as sets of imprimitivity.

Lemma 2.5 (Hall [5, Theorem 5.6.1, pp. 64–65]). Let the group $G$ act transitively on a set $X$ and let $B \subset X$. Then $B$ is a $G$-block if and only if there exists $H < G$ and $x \in X$ such that $B = Hx$ and $\text{Stab}_G(x) < H < G$.

Lemma 2.6. Let $\mathbb{Z}_{p^2}$ act regularly on a set $X$ and let $B \subset X$. Let $H = \langle p \rangle$ be the unique subgroup of $\mathbb{Z}_{p^2}$ of order $p$. Then, $B$ is a $\mathbb{Z}_{p^2}$-block if and only if there exists $x \in X$ such that $B = Hx$. In other words, each $\mathbb{Z}_{p^2}$-block is an $H$-orbit $Hx$ for some $x \in X$. In particular, if the intersection of two blocks is not the empty set, the two blocks are equal.

Proof. Because $\mathbb{Z}_{p^2}$ acts regularly, we have $\text{Stab}_{\mathbb{Z}_{p^2}}(x) = e$ for each $x \in X$. By Lemma 2.5, the $\mathbb{Z}_{p^2}$-blocks are $H$-orbits $Hx$ for $x \in X$. □

Definition (Sabidussi [10]). Let $U$ and $V$ be sets, $H$ and $K$ groups of permutations of $U$ and $V$, respectively. The wreath product $H \wr K$ is the group of all permutations $f$ of $U \times V$ for which there exist $h \in H$ and an element $k_u$ of $K$ for each $u \in U$ such that

$$f(u, v) = (hu, k_u v)$$

for all $(u, v) \in U \times V$.

We use the following lemma that Sabidussi [10] states without proof. The lemma provides a connection between the wreath product of the automorphism groups of two graphs and the automorphism group of the lexicographic product of these two graphs. Sabidussi [10] and Anderson and Lipman [2] give necessary and sufficient conditions for equality to hold.

Lemma 2.7 (Sabidussi [10]). Let $U$ and $V$ be graphs. Then $\text{Aut}(U) \wr \text{Aut}(V)$ is contained in $\text{Aut}(U \text{ lex } V)$.
3. Proof of Main Theorem

3.1. Proof of $1 \Rightarrow 2$

Let $X = \text{Cay}(G : T)$ be a Cayley digraph on a group $G$ of order $p^2$, where $p$ is prime. Assume $X$ is isomorphic to a Cayley digraph on both $\mathbb{Z}_p^2$ and $\mathbb{Z}_p \times \mathbb{Z}_p$. We need to show there exists a subgroup $H$ of $G$ of order $p$ such that for every $t \in T \setminus H$, we have $tH \subseteq T$.

**Lemma 3.1.** Every Sylow $p$-subgroup of $\text{Aut}(X)$ contains a regular subgroup $Q$ isomorphic to $\mathbb{Z}_p$ and a regular subgroup $R$ isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. In particular, the order of every Sylow $p$-subgroup is at least $p^3$.

**Proof.** From Theorem 2.1, the group $\text{Aut}(X)$ contains a regular subgroup $Q'$ isomorphic to $\mathbb{Z}_p$. From the Sylow theorems [5, Corollary 4.2.1, p. 45], there exists a Sylow $p$-subgroup of $\text{Aut}(X)$ that contains $Q'$. Since Sylow $p$-subgroups are conjugate in a finite group $G$, every Sylow $p$-subgroup of $\text{Aut}(X)$ contains a conjugate $Q$ of $Q'$, which is also a regular subgroup isomorphic to $\mathbb{Z}_p$. Similarly, every Sylow $p$-subgroup of $\text{Aut}(X)$ contains a regular subgroup $R$ isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. Since $Q$ is not isomorphic to $R$, the order of every Sylow $p$-subgroup is at least $p^3$. □

Let $P$ be a Sylow $p$-subgroup of $\text{Aut}(X)$. From Lemma 3.1, the subgroup $P$ contains a regular subgroup $Q$ isomorphic to $\mathbb{Z}_p$ and a regular subgroup $R$ isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. From Lemma 2.6, we know that $Q$-blocks exist. Let $B_1$ and $B_2$ be distinct $Q$-blocks and let $b_1 \in B_1$ such that $b_1$ is adjacent to some vertex $b_2$ in $B_2$. We will show that $b_1$ is adjacent to every vertex in $B_2$. The two main steps are showing that $\text{Stab}_P(b_1)$ moves $b_2$ to $p$ vertices and then showing that $\text{Stab}_P(b_1)$ moves $b_2$ only within $B_2$.

**Lemma 3.2.** For every vertex $x$ in $V(X)$, we have $|\text{Stab}_P(x)| > 1$.

**Proof.** From Lemma 2.3, we have

$$[P: \text{Stab}_P(x)] = |P\text{-orbit of } x|.$$ 

By Lemma 3.1, $P$ is transitive, so we have $[P: \text{Stab}_P(x)] = p^2$. Assume $|\text{Stab}_P(x)| = 1$, which implies that $|P| = p^2$ in contradiction to Lemma 3.1. □

**Lemma 3.3.** We have $|\text{Stab}_P(b_1)-\text{orbit of } b_1| = p$.

**Proof.** By Lemma 2.3, the size of the $\text{Stab}_P(b_1)$-orbit of $b_2$ must divide the order of $\text{Stab}_P(b_1)$, which is a power of $p$. Furthermore, since $\text{Stab}_P(b_1) \subseteq P$, we see that

$$|\text{Stab}_P(b_1)-\text{orbit of } b_2| \leq |P\text{-orbit of } b_2| = p^2.$$ 

It suffices to show $|\text{Stab}_P(b_1)-\text{orbit of } b_2|$ is neither $p^2$ nor 1.
Step 1: We show $|\text{Stab}_p(b_1)\text{-orbit of } b_2| \neq p^2$. Assume for the sake of a contradiction that $|\text{Stab}_p(b_1)\text{-orbit of } b_2| = p^2$ which implies that the $P$-orbit of $b_2$ equals the $\text{Stab}_p(b_1)$-orbit of $b_2$. Since $b_1$ is in the $P$-orbit of $b_2$, we also have $b_1$ in the $\text{Stab}_p(b_1)$-orbit of $b_2$ which contradicts the fact that $b_1$ and $b_2$ were fixed in different blocks.

Step 2: We show $|\text{Stab}_p(b_1)\text{-orbit of } b_2| \neq 1$. Assume for the sake of a contradiction that $|\text{Stab}_p(b_1)\text{-orbit of } b_2| = 1$. Then every element of $\text{Stab}_p(b_1)$ fixes $b_2$, so $\text{Stab}_p(b_1) \subseteq \text{Stab}_p(b_2)$. On the other hand, from Lemma 2.4, we have $|\text{Stab}_p(b_2)| = |\text{Stab}_p(b_1)|$. Thus, we have $\text{Stab}_p(b_1) = \text{Stab}_p(b_2)$.

The group $P$ is transitive, so there exists $h \in P$ such that $hb_1 = b_2$. From Lemma 2.4, have $h\text{Stab}_p(b_1)h^{-1} = \text{Stab}_p(b_2)$. Since $\text{Stab}_P(b_1) = \text{Stab}_P(b_2)$, this implies that $h$ belongs to the normalizer $N$ of $\text{Stab}_P(b_1)$. With $hb_1 = b_2$, we have $b_1$ and $b_2$ in the same $N$-orbit.

The group $P$ is transitive, so the subgroup $\text{Stab}_p(b_1)$ is a proper subgroup of $P$, which implies that $\text{Stab}_p(b_1)$ is not its own normalizer [5, p. 176]. We also show that $N \neq P$. To this end, assume for the sake of a contradiction that $N = P$. By Lemma 2.4, the stabilizer in $P$ of any element in $V(X)$ is a conjugate of $\text{Stab}_p(b_1)$. By assumption, $\text{Stab}_p(b_1)$ is normal in $P$, so every stabilizer is equal to $\text{Stab}_p(b_1)$. Thus, $\text{Stab}_p(b_1)$ fixes every element of $V(X)$. The identity permutation is the only permutation which fixes every element in $X$. So we have $|\text{Stab}_p(b_1)| = 1$, which contradicts Lemma 3.2. Thus, $N \neq P$.

Then, $N$ is a proper subgroup of $P$ that properly contains $\text{Stab}_p(b_1)$. We have $\text{Stab}_p(b_1) < N < P$ which by Lemma 2.5 implies that the $N$-orbit $Nb_1$ is a $P$-block. Since $Q \subseteq P$, the $P$-block $Nb_1$ is also a $Q$-block. Since $b_2$ is also in the $N$-orbit of $b_1$, the vertex $b_2$ is also in $Nb_1$, a $Q$-block. Therefore, by Lemma 2.6, since the intersection of $Nb_1$ and $B_1$ contains $b_1$, the two blocks are equal. Thus, $b_2$ is also in $B_1$ which is a contradiction since we chose $b_1$ and $b_2$ from different $Q$-blocks.

Lemma 3.4. For every $x \in V(X)$, there is a $P$-block that contains $x$.

Proof. From Lemma 3.1, $\text{Stab}_P(x)$ has index $p^2$ in $P$. So the subgroup $\text{Stab}_P(x)$ is properly contained in a maximal subgroup $M$ that has index $p$ in $P$ [5, Theorem 4.3.2, p. 48]. Since $\text{Stab}_P(x) < M < P$, Lemma 2.5 asserts that $Mx$ is a $P$-block. It is clear that $Mx$ contains $x$. □

Lemma 3.5. Every $Q$-block is a $P$-block.

Proof. Since $Q$ is isomorphic to $Z_{p^r}$, there exists only one subgroup $H$ of $Q$ of order $p$. By Lemma 2.6, we need to show that the $H$-orbits are $P$-blocks. Let $B$ be a $P$-block. Since $Q \subseteq P$, every $P$-block is a $Q$-block, so $B$ is also a $Q$-block. By Lemma 2.6, only the $H$-orbits are $Q$-blocks. Thus, $B$ is an $H$-orbit as desired. □

Lemma 3.6. Every $Q$-block is an $R$-block.
Proof. By Lemma 3.5, every $Q$-block is a $P$-block. Since $R \subset P$, every $P$-block is also an $R$-block. □

Lemma 3.7. The $\text{Stab}_P(b_1)$-orbit of $b_2$ is $B_2$.

Proof. From Lemma 3.5, the $Q$-blocks $B_1$ and $B_2$ are $P$-blocks. We first show that $SB_2 = B_2$ where $S = \text{Stab}_P(b_1)$. From Lemma 2.5, there exists a proper subgroup $K$ of $P$ and $x \in V(X)$ such that $S < K$ and $Kx = B_1$. Let $g \in P$ such that $gB_1 = B_2$. Since $S$ is of index $p^2$ in $P$, then $K$ is of index $p$ in $P$, which implies $K$ is normal. Therefore, we have $S < K = gKn^{-1}$, which implies that $SgK = K$. Consequently, we have $g^{-1}SgK = K$, which yields $S(gK) = gK$ and therefore, $SB_2 = B_2$ as desired. Then, since $b_2 \in B_2$, the $S$-orbit of $b_2$ is contained in $B_2$. By Lemma 2.6, we have $|B_2| = p$ and by Lemma 3.3, we have $|S$-orbit of $b_2| = p$. Thus, we see that the $S$-orbit of $b_2$ is $B_2$ as desired. □

Lemma 3.8. The vertex $b_1$ is adjacent to every vertex in $B_2$.

Proof. Recall that $b_1$ is adjacent to $b_2$, which is in $B_2$. We note that $\text{Stab}_P(b_1) \subset \text{Aut}(X)$, so for every $s \in \text{Stab}_P(b_1)$, we have $sb_1$ adjacent to $sb_2$. Thus, we have $b_1 = sb_1$ adjacent to every vertex in the $\text{Stab}_P(b_1)$-orbit of $b_2$. By Lemma 3.7, the $\text{Stab}_P(b_1)$-orbit of $b_2$ is $B_2$, so $b_1$ is adjacent to every vertex in $B_2$ as desired. □

Lemma 3.9. There exists a subgroup $H$ of $G$ of order $p$ such that if a vertex $v$ in one coset of $H$ is adjacent to a vertex $w$ in a different coset of $H$, then $v$ is adjacent to all vertices in the coset of $H$ that contains $w$.

Proof. We consider two cases. First, let $G \cong \mathbb{Z}_p^r$. Then by Corollary 2.2, we may assume that $Q$ is the left regular representation of $G$. Let $H$ be the unique subgroup of $G$ of order $p$. We note that cosets of $H$ are $H$-orbits in the left regular representation of the group $G$. Then by Lemma 2.6, we know that cosets of $H$ are $Q$-blocks. Since $v$ and $w$ are in different blocks and $v$ is adjacent to $w$, we may assume that $b_1 = v$ and $b_2 = w$ where $B_1$ is $HV$ and $B_2$ is $HW$. By Lemma 3.8, we conclude that $v = b_1$ is adjacent to every vertex in $B_2$, which is $HW$ as desired. Second, let $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Then by Corollary 2.2, we may assume $R$ is the left regular representation of $G$. From Lemma 3.6, we know that the $Q$-block $B_1$ is an $R$-block. Then, from Lemma 2.5 there exists a subgroup $H$ of $G$ of order $p$ such that $B_1$ is an $H$-orbit. Thus, there exists $x \in G$ such that $Hx$ is a $Q$-block. By Lemma 3.5, we note that $Hx$ is a $P$-block. We claim that each coset $Hy$ of $H$ is a $Q$-block. Since $R$ is transitive, there exists $r \in R$ such that $y = rx$. Then, because $R$ is abelian, we have $Hy = Hrx = rHx$, which is a translate of $Hx$. Since translates of blocks are blocks, we conclude that $Hy$ is a $P$-block. Then, since $Q \subset P$, we see that $Hy$ is a $Q$-block as desired. Since $HV$ and $HW$ are distinct $Q$-blocks, we may assume $b_1 = v$ and $b_2 = w$ where $B_1$ is $HV$ and $B_2$ is $HW$. By Lemma 3.8, we conclude that $v = b_1$ is adjacent to every vertex in $B_2$, which is $HW$ as desired. □
Lemma 3.10. There exists a subgroup $H$ of $G$ of order $p$ such that for every $t \in T \setminus H$, we have $tH \subseteq T$.

Proof. Let $H$ be the subgroup described in Lemma 3.9. Given $t \in T \setminus H$. Choose $v \in G$ and let $w = vt$. We note that $v$ and $w$ are in different cosets of $H$ and $v$ is adjacent to $w$. By Lemma 3.9, we have $v$ adjacent to every vertex in the coset of $H$ that contains $w$. Thus, by definition of a Cayley digraph, we have $v^{-1}w \in T$ for every $w$ in $Hv$. Then, we see that $T$ contains $v^{-1}(Hw) = v^{-1}wH = tH$. □

3.2. Proof of 2 ⇒ 3

We want to prove that $X$ is isomorphic to a lexicographic product of Cayley digraphs on $\mathbb{Z}_p$. Because the following result may be of independent interest, we begin with a lemma about general digraphs. We later apply the lemma to Cayley digraphs.

Lemma 3.11. Let $X$ and $\bar{X}$ be digraphs. Let $\varphi: V(X) \rightarrow V(\bar{X})$ be a surjective map. Assume the following conditions are satisfied:

1. For every $v$ and $w$ in $V(X)$, the induced subdigraph $X[\varphi^{-1}v]$ is isomorphic to the induced subdigraph $\bar{X}[\varphi^{-1}w]$.
2. For every $x$ and $y$ in $V(X)$ with $\varphi x \neq \varphi y$, the vertex $x$ is adjacent to the vertex $y$ in $X$ if and only if $\varphi x$ is adjacent to $\varphi y$ in $\bar{X}$.

Then $X \cong \bar{X} \text{lex } X[\varphi^{-1}v_0]$ for every $v_0 \in V(\bar{X})$.

Remark. A digraph homomorphism is a map $\varphi$ from $V(X)$ onto $V(Y)$ such that if $x$ is adjacent to $y$, then $\varphi x$ is adjacent to $\varphi y$. Condition (2) also requires the converse to be true. Because we assume the digraphs have no loops, we have the restriction $\varphi x \neq \varphi y$ in condition (2).

Proof. Choose some $v_0 \in \bar{X}$. By Condition (1), for each $v = \varphi x \in \bar{X}$, we can choose a digraph isomorphism $m_{\varphi x}$ from $X[\varphi^{-1}v]$ to $X[\varphi^{-1}v_0]$. Define the function $L: X \rightarrow \bar{X} \text{lex } X[\varphi^{-1}v_0]$ by $Lx = (\varphi x, m_{\varphi x}x)$.

It is straightforward to check that $L$ is a digraph isomorphism. □

Let $X = \text{Cay}(G : T)$ be a Cayley digraph on a group $G$ of order $p^2$, where $p$ is prime. Assume there is a subgroup $H$ of $G$ of order $p$, such that for every $t \in T \setminus H$, we have $tH \subseteq T$. We must show that there exist Cayley digraphs $U$ and $V$ on $\mathbb{Z}_p$ such that $X \cong U \text{ lex } V$.

Construct the digraph $\bar{X}$ as follows. The vertex set $V(\bar{X})$ is the set $\{Hx \mid x \in G\}$ of cosets of $H$ in $G$. The edge set $E(\bar{X})$ is the set $\{[Hx, Hy] \mid x^{-1}y \in T \setminus H\}$. Thus, $Hx$ is adjacent to $Hy$ if and only if there exists $x_0 \in Hx$ and $y_0 \in Hy$ such that $x^{-1}_0 y_0 \in T \setminus H$.

We avoid loops in the digraph $\bar{X}$ with the condition that $x^{-1}y$ not be in $H$.

Lemma 3.12. The digraph $\bar{X}$ is isomorphic to a Cayley digraph on $\mathbb{Z}_p$. 
Proof. Let $\tilde{G} = \text{right cosets of } H \text{ in } G$ and $\tilde{T} = \{Ht \mid t \in T \setminus H\}$. Given $\tilde{g}_1$ and $\tilde{g}_2$ in $\tilde{G}$, by definition $\tilde{g}_1$ is adjacent to $\tilde{g}_2$ in $\tilde{X}$ if and only if $\tilde{g}_1^{-1} \tilde{g}_2 \in \tilde{T}$. So by definition of a Cayley digraph, it is clear that $\tilde{X} = \text{Cay}(\tilde{G} : \tilde{T})$. Since $H$ is a normal subgroup of index $p$ in $G$, we have $\tilde{G} \cong \mathbb{Z}_p$. Thus,

$$\tilde{X} = \text{Cay}(\tilde{G} : \tilde{T}) \cong \text{Cay}(\mathbb{Z}_p : \tilde{T}) \quad \square$$

Lemma 3.13. The subdigraph $X[H]$ induced by $H$ is isomorphic to a Cayley digraph on $\mathbb{Z}_p$.

Proof. We show that $X[H] = \text{Cay}(H : T \cap H)$. The vertices of $X[H]$ are the elements of $H$. Let $x$ and $y$ be in $H$. In $X[H]$, we have $x$ adjacent to $y$ if and only if $x^{-1}y \in T$. Since $x, y \in H$, this means $x$ is adjacent to $y$ if and only if $x^{-1}y \in T \cap H$. Since $H \cong \mathbb{Z}_p$, we have

$$X[H] = \text{Cay}(H : T \cap H) \cong \text{Cay}(\mathbb{Z}_p : T \cap H) \quad \square$$

Let $\varphi$ be the natural surjective map, $\varphi x = Hx$, from $V(X)$ onto $V(\tilde{X})$. From Lemmas 3.11–3.13, it suffices to show $\varphi$ satisfies the conditions of Lemma 3.11.

Step 1: For every $\tilde{x}$ and $\tilde{y}$ in $V(\tilde{X})$, the subdigraph $X[\varphi^{-1}\tilde{x}]$ is isomorphic to the induced subdigraph $X[\varphi^{-1}\tilde{y}]$. Each inverse image $\varphi^{-1}\tilde{x}$ is a coset of $H$. For each $x \in G$, it is straightforward to check that the map $\gamma$, defined by $\gamma h = hx$, from $X[H]$ to $X[Hx]$ is an isomorphism. The proof is similar to the proof of Corollary 2.2.

Step 2. Given $x$ and $y$ in $X$ with $\varphi x \neq \varphi y$, we have $x$ adjacent to $y$ if and only if $\varphi x$ is adjacent to $\varphi y$. Because $X = \text{Cay}(G : T)$, we have $x$ adjacent to $y$ if and only if $x^{-1}y \in T$. Because $\varphi x \neq \varphi y$, we have $x^{-1}y \notin H$. Thus, we see that $x^{-1}y \notin T$ implies that $x^{-1}y \notin T \setminus H$. By our assumption, for every $t \in T \setminus H$, we have $tH \subseteq T$. Thus, since $G$ is abelian, we note that for every $t \in T$ and $h_1, h_2 \in H$, we have $t \in T \setminus H$ if and only if $h_1th_2 \in T \setminus H$. Therefore, we have $x^{-1}y \notin T \setminus H$ if and only if there exists $x_0 \in Hx$ and $y_0 \in Hy$ such that $x_0^{-1}y_0 \in T \setminus H$. Thus, by the definition of $\tilde{X}$, we have $x$ adjacent to $y$ if and only if $\varphi x$ is adjacent to $\varphi y$. $\square$

3.3. Proof of $3 \Rightarrow 1$

Let $X = \text{Cay}(G : T)$ be a Cayley digraph on a group $G$ of order $p^2$, where $p$ is prime. Assume there exist Cayley digraphs $U$ and $V$ of $\mathbb{Z}_p$ such that $X \cong U \text{ lex } V$. We show that the digraph $X$ is isomorphic to a Cayley digraph on both $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.

Because $U$ and $V$ are Cayley digraphs on $\mathbb{Z}_p$, the vertex set of each of these digraphs is $\mathbb{Z}_p$. Thus, we may define a permutation $h$ of the vertices of $U$ by $h(u) = u + 1$, and we may define a permutation $k$ of the vertices of $V$ by $k(v) = v + 1$. It is clear that $h$ and $k$ are $p$-cycles. It is easy to check that $h$ is an automorphism of $U$ and $k$ is an automorphism of $V$. Let $H = \langle h \rangle$ and let $K = \langle k \rangle$. It is clear that $H$ is a regular subgroup of $\text{Aut}(U)$ and $K$ is a regular subgroup of $\text{Aut}(V)$. 


By Lemma 2.7, we have $\text{Aut}(U \wr \text{Aut}(V)) \subseteq \text{Aut}(U \leq V)$. Since $H \subseteq \text{Aut}(U)$ and $K \subseteq \text{Aut}(V)$, the wreath product $H \wr K$ is contained in $\text{Aut}(U) \wr \text{Aut}(V)$.

To show that $X$ is isomorphic to a Cayley graph on both groups of order $p^2$, by Theorem 2.1 it suffices to prove that $H \wr K$ contains a regular subgroup isomorphic to $\mathbb{Z}_{p^2}$ and a regular subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

**Lemma 3.14.** The wreath product $H \wr K$ contains a regular subgroup isomorphic to $\mathbb{Z}_{p^2}$ and a regular subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

**Proof.** We define a permutation $f \in H \wr K$ as follows. Given any element $(u, v)$ of $U \times V$, we let

$$f(u, v) = (hu, ku v),$$

where $h$ is the $p$-cycle defined above and $k_u = k$ if $u = 0$ and $k_u = e$ if $u \neq 0$. Thus, we see that

$$f(u, v) = \begin{cases} (u + 1, v) & \text{if } u \neq p - 1, \\ (u + 1, v + 1) & \text{if } u = p - 1. \end{cases}$$

Note that the permutation $f$ always adds one to $u$ and if $u = p - 1$, it also adds one to $v$. All addition is done modulo $p$.

It is trivial to show that $f$ is a cycle of length $p^2$ and, thus, we see $\langle f \rangle$ is a regular group isomorphic to $\mathbb{Z}_{p^2}$ as required.

Define the permutations $\bar{f}$ and $\bar{g}$ as follows. Given any element $(u, v)$ of $U \times V$, let

$$\bar{f}(u, v) = (u + 1, v)$$

and let

$$\bar{g}(u, v) = (u, v + 1).$$

Both $\bar{f}$ and $\bar{g}$ generate groups of order $p$ and are in $H \wr K$. Clearly, the group $\langle \bar{f}, \bar{g} \rangle$ is regular and isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. □

**Acknowledgements**

I would like to thank my advisor Dave Witte. In addition, I would like to thank Daniel Goldstein for several ideas on how to approach this problem.

**References**

267–270.
Berlin, 1980.
405–434.
136–145.
293–304.