Isomorphism Theorem for Cayley Graphs of Semigroup of Integer Modulo Prime Power Relative to an Invertible Element

Ekkachai Laysirikul

Department of Mathematics, Faculty of Science, Naresuan University, Phitsanulok 65000
Corresponding author. E-mail address: ekkachail@nu.ac.th
Received: 18 January 2019; Accepted: 3 April 2019

Abstract

Let p be a prime number and $a, k \in \mathbb{N}$ such that $\gcd(a,p) = 1$. We denote the semigroup of integers modulo p^k under usual multiplication by $\mathbb{Z}_{p^k}$. Then, the Cayley graph of $\mathbb{Z}_{p^k}$ relative to $\bar{a}$ is the digraph $Cay(\mathbb{Z}_{p^k}, \bar{a})$, where

$$V\left(Cay(\mathbb{Z}_{p^k}, \bar{a})\right) = \mathbb{Z}_{p^k} \text{ and } (\bar{x}, \bar{y}) \in E\left(Cay(\mathbb{Z}_{p^k}, \bar{a})\right) \text{ if and only if } \bar{y} = \bar{x}\bar{a}.$$

In this paper, we describe the characterization of $Cay(\mathbb{Z}_{p^k}, \bar{a})$. Our objective is to investigate the isomorphism theorem between two Cayley graphs of $\mathbb{Z}_{p^k}$ relative to $\bar{a}$ and $\bar{b}$, respectively, where a and b are both relatively prime to p.

Keywords: Cayley graph, integer modulo, isomorphism, prime number, semigroup, digraph

Introduction

In 1878, Arthur Cayley introduce the notion of Cayley graph for representing the structure of abstract groups which are described by their generators. The theory of Cayley graphs has been grown into a substantial branch in algebraic graph theory. It has relations with some classical problems in pure mathematics and many researchers have paid their attentions to this structure see Konstantinova (2008).

Let Γ be a digraph, where $V(\Gamma)$ is the set of vertices and $E(\Gamma)$ the set of edges of Γ which is a subset of $V(\Gamma) \times V(\Gamma)$. An edge joins the initial vertex u to the terminal vertex v is denoted by (u, v). For a semigroup G and a non-empty subset S of G, the Cayley graph of G relative to S is denoted by $Cay(G, S)$, which is a digraph with vertex set G and (x, y) is an edge of $Cay(G, S)$ if and only if $y = xs$ for some $s \in S$. In this case, we called S is the connection set and write $Cay(G, a)$ instead of $Cay(G, \{a\})$.

Hosseinzadeh and Assari (2014) considered some operations of Cayley graphs on semigroups. They have described graph's properties which constructed from the interesting operations. Later, Suksumran and Panma (2015) gave a condition to determine whether or not a Cayley graph of a semigroup is strongly connected and also characterized weakly connected Cayley graphs of a semigroup. And Khosravi (2016) gave characterization for Cayley graphs of cancellative semigroup and he gave a criterion to check whether a digraph is a Cayley graph of a cancellative semigroup. Kelarev and Praeger (2003) studied the transitivity properties of Cayley graph.

In this study, we let $\mathbb{Z}_{p^k}$ be the set of all integer modulo p^k where p is a prime number and k is a positive integer. It is well-known that $\mathbb{Z}_{p^k}$ forms a semigroup under the multiplication. The aim of this paper is to prove isomorphism theorem between $Cay(\mathbb{Z}_{p^k}, \bar{a})$ and $Cay(\mathbb{Z}_{p^k}, \bar{b})$ where $\bar{a}, \bar{b} \in \mathbb{Z}_{p^k}$ and $\gcd(a,p) = \gcd(b,p) = 1$.

Now, we remind some notions that will be used in our study. In this paper, we denote the set of all natural numbers by $\mathbb{N}$. For two relatively prime positive integers a and n, the least positive integers x such that $a^x \equiv 1 (\mathrm{mod}\, n)$ is called the *order of a modulo n*. We denote the order of a modulo n by $ord_n a$. Moreover, we

obtain that the integer a^{x-1} satisfies the equality $a(a^{x-1}) \equiv 1(\mathrm{mod}\ n)$ and it is called an inverse of a modulo n. We denote the congruence class of a modulo n by $\bar{a}$.

Proposition 1. Let $p, k \in \mathbb{N}$ such that p be a prime number and $l, m \in \{0,1,2, \dots, k-1\}$ with $l < m$. If $\bar{a} \in \mathbb{Z}_{p^k}$ such that $\gcd(a,p) = 1$. Then $ord_{p^{k-m}} a \leq ord_{p^{k-l}} a$.

Proof. It follows directly from the fact that $p^{k-m} | p^{k-l}$.

Proposition 2. Let $m, p, k \in \mathbb{N}$ be such that p is a prime number and $m < k$. Then

$$|\{b \in N : \gcd(b, p^k) = p^m\}| = p^{k-m} - p^{k-(m+1)} \text{ where } N = \{1,2,3, \dots, p^k\}.$$

Proof. Let $T = \{b \in N : \gcd(b, p^k) = p^m\}$. Note that $T = \{b \in N : p^m | b\} \setminus \{b \in N : p^{m+1} | b\} = \left\{p^m x : x \in \{1,2, \dots, p^{k-m}\}\right\} \setminus \left\{p^{m+1} x : x \in \left\{1,2, \dots, p^{k-(m+1)}\right\}\right\}$. Thus $|T| = p^{k-m} - p^{k-(m+1)}$.

Theorem 3. Let $a, b, c \in \mathbb{Z}$ with $0 < b$. Then there exist unique integers q and r satisfying

$$a = bq + r \text{ and } c \leq r < b + c.$$

For a subgraph Γ of a Cayley graph $Cay(G, S)$ and an element a in a semigroup G, we define a digraph $a\Gamma$ by $V(a\Gamma) = \{ax : x \in V(\Gamma)\}$ and $E(a\Gamma) = \{(ax, ay) : (x, y) \in E(\Gamma)\}$.

Main Results

From now on, we let $a, p, k \in \mathbb{N}$ such that p is a prime number and $\gcd(a,p) = 1$. In this paper, we define the digraph $P_{0,1}$ by $V(P_{0,1}) = \langle \bar{a} \rangle = \{\bar{a}^n : n \in \mathbb{N}\}$ and $E(P_{0,1}) = \{(\bar{a}^n, \bar{a}^{n+1}) : n \in \mathbb{N}\}$. For each $i \in \{0, 1, 2, \dots, k-1\}$ and $j \in \mathbb{N}$, define $P_{i,j} = \bar{a}_{i,j} P_{0,1}$ where $\bar{a}_{i,1} = \bar{p}^i$ and $\bar{a}_{i,j} \in \mathbb{Z}_{p^k} \setminus \bigcup_{l=1}^{j-1} V(P_{i,l})$ and $\gcd(a_{i,j}, p^k) = p^i$. In the rest of this paper, we denote the digraph $Cay(\mathbb{Z}_{p^k}, \bar{a})$ without vertex $\bar{0}$ and without an edge $(\bar{0}, \bar{0})$ by $Cay^*(\mathbb{Z}_{p^k}, \bar{a})$.

Theorem 4. Let n_i be the smallest positive integer such that

$$\left\{\bar{x} \in \mathbb{Z}_{p^k} \setminus \bigcup_{l=1}^{n_i} V(P_{i,l}) : \gcd(x, p^k) = p^i\right\} = \emptyset \text{ for each } i \in \{0,1,2 \dots, k-1\}.$$

Then $Cay^*(\mathbb{Z}_{p^k}, \bar{a}) = \bigcup_{i=1}^{k-1} \bigcup_{l=1}^{n_i} P_{i,l}$.

Proof. We note that if $a_{i,m}$ exists, then $\left\{\bar{x} \in \mathbb{Z}_{p^k} \setminus \bigcup_{l=1}^{m} V(P_{i,l}) : \gcd(x, p^k) = p^i\right\}$ is a proper subset of $\left\{\bar{x} \in \mathbb{Z}_{p^k} \setminus \bigcup_{l=1}^{n} V(P_{i,l}) : \gcd(x, p^k) = p^i\right\}$ for each positive integer n such that $n < m$. This implies that $\left\{\bar{x} \in \mathbb{Z}_{p^k} \setminus \bigcup_{l=1}^{n} V(P_{i,l}) : \gcd(x, p^k) = p^i\right\} = \emptyset$ for some $n \in \mathbb{N}$. Thus, n_i exists for each $i = 0,1, \dots, k-1$. Let $\Gamma = \bigcup_{i=0}^{k-1} \bigcup_{l=1}^{n_i} P_{i,l}$. Then it is clear that $V(\Gamma) \subseteq \mathbb{Z}_{p^k} \setminus \{\bar{0}\} = V\left(Cay^*(\mathbb{Z}_{p^k}, \bar{a})\right)$. We let $\bar{y} \in \mathbb{Z}_{p^k}$ be such that $\gcd(y, p^k) = p^i$ for some $i \in \{0, 1, 2, \dots, k-1\}$. Assume that $\bar{y} \notin \bigcup_{l=1}^{n_i} V(P_{i,l})$. Then $\bar{y} \in \mathbb{Z}_{p^k} \setminus \bigcup_{l=1}^{n_i} V(P_{i,l})$ and $\gcd(y, p^k) = p^i$. Hence, $\left\{\bar{x} \in \mathbb{Z}_{p^k} \setminus \bigcup_{l=1}^{n_i} V(P_{i,l}) : \gcd(x, p^k) = p^i\right\} \neq \emptyset$, which is a contradiction. Thus, $\bar{y} \in \bigcup_{l=1}^{n_i} V(P_{i,l})$, which implies $V(\Gamma) = V\left(Cay^*(\mathbb{Z}_{p^k}, \bar{a})\right)$.

Next, we will prove that $E\left(Cay^*(\mathbb{Z}_{p^k}, \bar{a})\right) = E(\Gamma)$. Let $(\bar{x}, \bar{y}) \in E(\Gamma)$. Then $(\bar{x}, \bar{y}) \in E(P_{i,j})$, where $i \in \{0, 1, 2, \dots, k-1\}$ and $j \in \{1,2,3, \dots, n_i\}$. Thus, $(\bar{x}, \bar{y}) = (\bar{a}_{i,j} \bar{a}^n, \bar{a}_{i,j} \bar{a}^{n+1})$, where $\bar{a}_{i,j} \in \mathbb{Z}_{p^k} \setminus \{\bar{0}\}$ and $n \in \mathbb{N}$. Hence, $(\bar{x}, \bar{y}) \in E\left(Cay^*(\mathbb{Z}_{p^k}, \bar{a})\right)$.

Finally, let $(\bar{x}, \bar{y}) \in E\left(Cay^*(\mathbb{Z}_{p^k}, \bar{a})\right)$, that is, $\bar{y} = \overline{xa}$. Form $\bar{x} \neq \bar{0}$, we suppose that $\gcd(x, p^k) = p^i$, where $i \in \{0, 1, 2, \dots, k-1\}$. It follows from above that $\bar{x} \in V(P_{i,j})$ for some $j \in \{1,2,3, \dots, n_i\}$. Then $\bar{x} = \bar{a}_{i,j} \bar{a}^n$ and $\bar{y} = \bar{a}_{i,j} \bar{a}^{n+1}$ for some $n \in \mathbb{N}$. Since $(\bar{a}^n, \bar{a}^{n+1}) \in E(P_{0,1})$, we obtain $(\bar{x}, \bar{y}) = (\bar{a}_{i,j} \bar{a}^n, \bar{a}_{i,j} \bar{a}^{n+1}) \in E(\Gamma)$ and so $E\left(Cay^*(\mathbb{Z}_{p^k}, \bar{a})\right) = E(\Gamma)$. Thus the graphs $Cay^*(\mathbb{Z}_{p^k}, \bar{a})$ and Γ are equal.

Example 5. Consider $Cay(\mathbb{Z}_{16}, \bar{3})$.

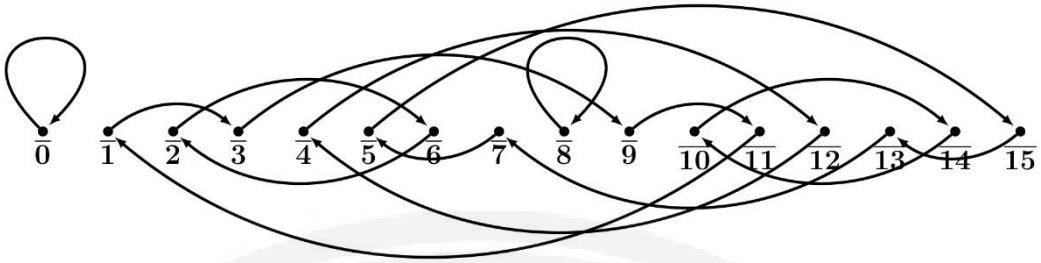

Figure 1 $Cay(\mathbb{Z}_{16}, \bar{3})$

From Theorem 4, we obtain that $Cay^*(\mathbb{Z}_{16}, \bar{3}) = P_{0,1} \cup P_{0,2} \cup P_{1,1} \cup P_{1,2} \cup P_{1,2} \cup P_{2,1} \cup P_{3,1}$.

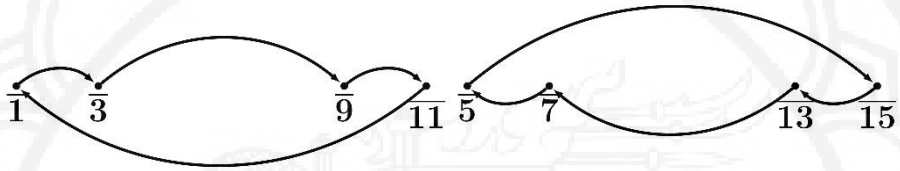

Figure 2 $P_{0,1}$ and $P_{0,2}$

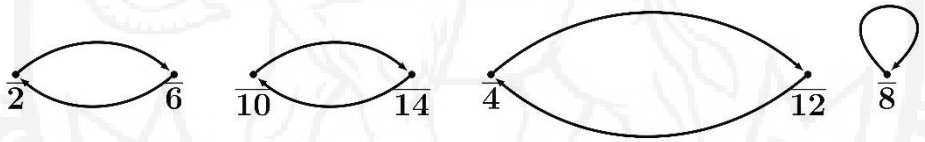

Figure 3 $P_{1,1}, P_{1,2}, P_{2,1}$ and $P_{3,1}$

Theorem 6. Let $l \in \{0, 1, 2, \ldots, k-1\}$. Then $ord_{p^{k-l}}a = |V(P_{l,1})|$.

Proof. Let $ord_{p^{k-l}}a = m$. We will show that $V(P_{l,1}) = \{\bar{p}^l\bar{a}, \bar{p}^l\bar{a}^2, \bar{p}^l\bar{a}^3, \ldots, \bar{p}^l\bar{a}^m\}$. Obviously, $\{\bar{p}^l\bar{a}, \bar{p}^l\bar{a}^2, \bar{p}^l\bar{a}^3, \ldots, \bar{p}^l\bar{a}^m\} \subseteq V(P_{l,1})$. Let $\bar{x} \in V(P_{l,1})$. Then $\bar{x} = \bar{p}^l\bar{a}^j$ for some $j \in \mathbb{N}$. Suppose that $m < j$. By Theorem 3, $j = mq + r$ for some $q, r \in \mathbb{Z}$ and $1 \leq r < m + 1$. Clearly, $1 \leq q$. Then $p^l a^j \equiv p^l a^{mq} \cdot a^r (\mathrm{mod}\ p^k)$. Hence, $a^j \equiv a^{mq} \cdot a^r \equiv 1 \cdot a^r = a^r \ (\mathrm{mod}\ p^{k-l})$ since $\gcd(p^l, p^k) = p^l$ and $ord_{p^{k-l}}a = m$. Therefore, $p^l a^j \equiv p^l a^r (\mathrm{mod}\ p^k)$, which implies $V(P_{l,1}) = \{\bar{p}^l\bar{a}, \bar{p}^l\bar{a}^2, \bar{p}^l\bar{a}^3, \ldots, \bar{p}^l\bar{a}^m\}$.

Next, we will prove that $|\{\bar{p}^l\bar{a}, \bar{p}^l\bar{a}^2, \bar{p}^l\bar{a}^3, \ldots, \bar{p}^l\bar{a}^m\}| = m$. Assume that $p^l a^j \equiv p^l a^i (\mathrm{mod}\ p^k)$, where $0 < i < j \leq m$. Since $\gcd(a^i p^l, p^k) = p^l$, we obtain that $a^{j-i} \equiv 1 \ (\mathrm{mod}\ p^{k-l})$. Hence $m \leq j - i$ since $ord_{p^{k-l}}a = m$. It is a contradiction. Thus, $\bar{p}^l\bar{a}^i \neq \bar{p}^l\bar{a}^j$ and then we get $ord_{p^{k-l}}a = |V(P_{l,1})|$.

Theorem 7. Let $l \in \{0,1,2, \ldots, k-1\}$ and $m, m' \in \{1,2,3,..,n_l\}$. If $V(P_{l,m}) \cap V(P_{l,m'}) \neq \emptyset$, then $P_{l,m} = P_{l,m'}$.

Proof. Suppose that $\bar{b} \in V(P_{l,m}) \cap V(P_{l,m'})$. Then there exist $h, h' \in \mathbb{N}$ such that $\bar{b} = \bar{a}_{l,m}\bar{a}^h$ and $\bar{b} = \bar{a}_{l,m'}\bar{a}^{h'}$. We assume that $h \leq h'$. From $\gcd(a, p) = 1$, we obtain that $a_{l,m} \equiv a_{l,m'}a^{h'-h} \ (\mathrm{mod}\ p^k)$. This implies that $V(P_{l,m}) \subseteq V(P_{l,m'})$. Similarly, we can verify that $V(P_{l,m'}) \subseteq V(P_{l,m})$ whence $P_{l,m} = P_{l,m'}$.

Theorem 8. Let $l \in \{0, 1, 2, \ldots, k-1\}$ and $m \in \{1,2,3, \ldots, n_l\}$. Then $P_{l,1}$ is isomorphic to $P_{l,m}$. Moreover,

$n_l = \frac{p^{k-l}-p^{k-(l+1)}}{ord_{p^{k-l}}a}$, where n_l is defined in Theorem 4.

Proof. Define $f : V(P_{l,1}) \to V(P_{l,m})$ by

$$f(\bar{p}^l\bar{a}^h) = \bar{a}_{l,m}\bar{a}^h \text{ for all } \bar{p}^l\bar{a}^h \in V(P_{l,1}).$$

Let $h, h' \in \mathbb{N}$ and suppose that $\bar{p}^l\bar{a}^h = \bar{p}^l\bar{a}^{h'}$. Since $\gcd(a_{l,m}, p^k) = p^l$, there exists $c \in \mathbb{Z}$ which satisfies $a_{l,m} = cp^l$ and $\gcd(c, p^k) = 1$. Hence,

$$f(\bar{p}^l\bar{a}^h) = \bar{a}_{l,m}\bar{a}^h = \overline{cp}^l\bar{a}^h = \overline{cp}^l\bar{a}^{h'} = \bar{a}_{l,m}\bar{a}^{h'} = f\left(\bar{p}^l\bar{a}^{h'}\right).$$

It follows that f is well- defined. Now, suppose that $f(\bar{p}^l\bar{a}^h) = f\left(\bar{p}^l\bar{a}^{h'}\right)$, then $\bar{a}_{l,m}\bar{a}^h = \bar{a}_{l,m}\bar{a}^{h'}$. Since $\gcd(c, p^k) = 1$ and $cp^la^h \equiv cp^la^{h'} (\mathrm{mod}\, p^k)$, we obtain that $p^la^h \equiv p^la^{h'} (\mathrm{mod}\, p^k)$. Therefore, f is injective. It is clear that f is a surjection and a graph homomorphism.

Now, we let $\bar{x} \in \{\bar{b} \in \mathbb{Z}_{p^k} : \gcd(b, p^k) = p^l\}$. Then we get $x \in \mathbb{Z}$, $\gcd(x, p^k) = p^l$ which implies $\bar{x} \in V(P_{l,j})$ for some $j \in \{1,2,3,\dots,n_l\}$. Therefore, $\bar{x} \in \bigcup_{m=1}^{n_l} V(P_{l,m})$. Let $\bar{y} \in \bigcup_{m=1}^{n_l} V(P_{l,m})$. Then $\bar{y} \in V(P_{l,j})$ for some $j \in \{1,2,3,\dots,n_l\}$. So $\bar{y} = \bar{a}_{l,j}\bar{a}^n$ for some $n \in \mathbb{N}$. Since $\gcd(a_{l,j}a^n, p^k) = p^l$, we get $\bar{y} \in \{\bar{b} \in \mathbb{Z}_{p^k} : \gcd(b, p^k) = p^l\}$ and hence $\{\bar{b} \in \mathbb{Z}_{p^k} : \gcd(b, p^k) = p^l\} = \bigcup_{m=1}^{n_l} V(P_{l,m})$. Note from Theorem 7 that $V(P_{l,m}) \cap V(P_{l,n}) = \emptyset$ if $n \neq m$. From Proposition 2 and $P_{l,1}$ is isomorphic to $P_{l,m}$, we have

$$p^{k-l} - p^{k-(l+1)} = |\bigcup_{m=1}^{n_l} V(P_{l,m})| = \sum_{m=1}^{n_l} |V(P_{l,m})| = |V(P_{l,1})|n_l.$$

Therefore, $p^{k-l} - p^{k-(l+1)} = (ord_{p^{k-l}}a)n_l$ via Theorem 6.

Theorem 9. Let $\bar{b} \in \mathbb{Z}_{p^k}$ be such that $\gcd(b, p) = 1$. Then $Cay(\mathbb{Z}_{p^k}, \bar{a})$ is isomorphic to $Cay(\mathbb{Z}_{p^k}, \bar{b})$ if and only if

$$ord_{p^{k-l}}a = ord_{p^{k-l}}b \text{ for all } l \in \{0, 1, 2, \dots, k-1\}.$$

Proof. From Theorem 4, we can suppose that $Cay^*(\mathbb{Z}_{p^k}, \bar{a}) = \bigcup_{i=1}^{k-1}\bigcup_{j=1}^{n_i} P_{i,j}$ and $Cay^*(\mathbb{Z}_{p^k}, \bar{b}) = \bigcup_{i=1}^{k-1}\bigcup_{j=1}^{n'_i} P'_{i,j}$. It is enough to suppose that $Cay^*(\mathbb{Z}_{p^k}, \bar{a})$ is isomorphic to $Cay^*(\mathbb{Z}_{p^k}, \bar{b})$. Let $l \in \{1,2,3,\dots,n'_i\}$. From Theorem 6, we will show $|V(P_{l,1})| = |V(P'_{l,1})|$ instead of $ord_{p^{k-l}}a = ord_{p^{k-l}}b$.

Assume that $f: V\left(Cay^*(\mathbb{Z}_{p^k}, \bar{a})\right) \to V\left(Cay^*(\mathbb{Z}_{p^k}, \bar{b})\right)$ is an isomorphism. From the definition of $P_{l,m}$, we note that two graphs $P_{l,m}$ and $P_{l',m'}$ are distinct or equal. Then $f\left(V(P_{l,1})\right) = V\left(P'_{l',i}\right)$ for some $l' \in \{0, 1, 2, \dots, k-1\}$ and $i \in \{1,2,3,\dots,n'_{l'}\}$. Since f is surjective, there exists $m \in \{0, 1, 2, \dots, k-1\}$ such that $f\left(V(P_{m,j})\right) = V(P'_{l,1})$ for some $j \in \{1,2,3,\dots,n_m\}$. There are four possible cases.

Case 1. $m, l' < l$. From Theorem 6, 8 and Proposition 1, we have

$$|V(P_{l,1})| \leq |V(P_{m,1})| = |V(P_{m,j})| = |V(P'_{l,1})| \leq \left|V\left(P'_{l',1}\right)\right| = \left|V\left(P'_{l',i}\right)\right| = |V(P_{l,1})|.$$

Case 2. $l < m, l'$. From Theorem 6, 8 and Proposition 1, we have

$$|V(P_{l,1})| = |V(P'_{l',i})| \leq |V(P'_{l,1})| = |V(P_{m,j})| \leq |V(P_{l,1})|.$$

Case 3. $m < l < l'$. We claim that there exist $s \in \{l, l+1, \dots, k-1\}$ and $d \in \{1, 2, 3, \dots, n_s\}$ such that $f\left(V(P_{s,d})\right) = V\left(P'_{r,d'}\right)$ for some $r \in \{0, 1, 2, \dots, l\}$ and $d' \in \{1, 2, 3, \dots, n'_r\}$. We suppose not. That is, for each $s \in \{l, l+1, \dots, k-1\}$ and $d \in \{1, 2, 3, \dots, n_s\}$, we have $f\left(V(P_{s,d})\right) = V\left(P'_{r,d'}\right)$ for some $r \in \{l+1, l+2, \dots, k-1\}$ and $d' \in \{1, 2, 3, \dots, n'_r\}$. From $V\left(Cay^*(\mathbb{Z}_{p^k}, \bar{a})\right)$ is finite and the injectivity of f, we obtain that

$$\left|\{V(P_{s,d}) : s = l, \dots, k-1 \text{ and } d = 1,2,\dots,n_s\}\right| < \left|\left\{V\left(P'_{r,d'}\right) : r = l, \dots, k-1 \text{ and } d' = 1,2,\dots,n'_r\right\}\right|.$$

We note from the prove of Theorem 8 that $\{\bar{c} \in \mathbb{Z}_{p^k} : \gcd(c, p^k) = p^h\} = \bigcup_{t=1}^{n_h} V(P_{h,t})$ for all $h \in \{0,1,2,\dots,k-1\}$. This implies that

$$\left|\{\bar{c} \in \mathbb{Z}_{p^k} : \gcd(c, p^k) = p^s \text{ and } s = l, \dots, k-1\}\right| = \left|\bigcup\{V(P_{s,d}) : s = l, \dots, k-1 \text{ and } d = 1,2,\dots,n_s\}\right|$$

$$< \left|\cup\left\{V\left(P'_{r,d'}\right) : r = l, \dots, k-1 \text{ and } d' = 1,2,\dots,n'_r\right\}\right|$$
$$= \left|\{\bar{c} \in \mathbb{Z}_{p^k} : \gcd(c,p^k) = p^r \text{ and } r = l,\dots,k-1\}\right|$$

which is a contradiction. Therefore, there exist $s \in \{l, l+1, \dots, k-1\}$ and $d \in \{1,2,3,\dots,n_s\}$ such that $f\left(V(P_{s,d})\right) = V\left(P'_{r,d'}\right)$ for some $r \in \{0,1,2,\dots,l\}$ and $d' \in \{1,2,3,\dots,n'_r\}$. From Theorem 6, 8 and Proposition 1, we have

$$|V(P_{l,1})| = |V(P'_{l',i})| \le |V(P'_{l,1})| \le \left|V\left(P'_{r,d'}\right)\right| = |V(P_{s,d})| \le |V(P_{l,1})|.$$

Case 4. $l' < l < m$. Similarly, there exist $s \in \{0,1,2,\dots,l\}$ and $d \in \{1,2,3,\dots,n_s\}$ such that $f\left(V(P_{s,d})\right) = V\left(P'_{r,d'}\right)$ for some $r \in \{l+1,\dots,k-1\}$ and $d' \in \{1,2,3,\dots,n'_r\}$. From Theorem 6, 8 and Proposition 1, we have

$$|V(P_{l,1})| \le |V(P_{s,d})| = \left|V\left(P'_{r,d'}\right)\right| \le |V(P'_{l,1})| = |V(P_{m,j})| \le |V(P_{l,1})|.$$

From four cases, we get $ord_{p^{k-l}}a = |V(P_{l,1})| = |V(P'_{l,1})| = ord_{p^{k-l}}b$. Clearly, if $m = l$ or $l' = l$, then $|V(P_{l,1})| = |V(P'_{l,1})|$. Thus, $ord_{p^{k-l}}a = ord_{p^{k-l}}b$ for each $l \in \{0,1,2,\dots,k-1\}$.

Suppose that $ord_{p^{k-l}}a = ord_{p^{k-l}}b$ for all $l \in \{0,1,2,\dots,k-1\}$. This means that $|V(P_{l,1})| = |V(P'_{l,1})|$ from Theorem 6. It is enough to verify that $Cay^*(\mathbb{Z}_{p^k}, \bar{a})$ is isomorphic to $Cay^*(\mathbb{Z}_{p^k}, \bar{b})$. Define $g : V\left(Cay^*(\mathbb{Z}_{p^k}, \bar{a})\right) \to V\left(Cay^*(\mathbb{Z}_{p^k}, \bar{b})\right)$ by

$$g(\bar{a}_{i,j}\bar{a}^h) = \bar{b}_{i,j}\bar{b}^h, \text{ where } i \in \{0,1,2,\dots,k-1\},\ j \in \{1,2,3,\dots,n_l\} \text{ and } h \in \mathbb{N}.$$

It follows from Theorem 8 and our assumption that $n_i = n'_i$ for all $i \in \{0,1,2,\dots,k-1\}$. Suppose that $\bar{a}_{s,r}\bar{a}^h = \bar{a}_{x,y}\bar{a}^{h'}$, where $h, h' \in \mathbb{N}$, $s, x \in \{0,1,2,\dots,k-1\}, r \in \{1,2,3,\dots,n_s\}$ and $y \in \{1,2,3,\dots,n_x\}$. Since $\bar{a}_{s,r}\bar{a}^h \in V(P_{s,r})$, $\bar{a}_{x,y}\bar{a}^{h'} \in V(P_{x,y})$, we get that $P_{s,r} = P_{x,y}$ and so $s = x$ and $r = y$. Thus $\bar{a}_{s,r} = \bar{a}_{x,y}$ and $\bar{b}_{s,r} = \bar{b}_{x,y}$. Since $a_{s,r}a^h \equiv a_{s,r}a^{h'} \pmod{p^k}$ and $\gcd(a_{s,r}, p^k) = p^s$, we then have $a^h \equiv a^{h'} \pmod{p^{k-s}}$. Suppose that $h < h'$, then we obtain $1 \equiv a^{h'-h} \pmod{p^{k-s}}$ since $\gcd(a,p) = 1$. Let $ord_{p^{k-s}}a = m = ord_{p^{k-s}}b$ so $m|(h'-h)$. There exists $c' \in \mathbb{N}$ such that $mc' + h = h'$. Then we have

$$b^{h'} = b^{mc'+h} = b^{mc'}b^h \equiv b^h \pmod{p^{k-s}}.$$

From $\gcd(b_{s,r}, p^k) = p^s$ and $\bar{b}_{s,r} = \bar{b}_{x,y}$, we deduce that $b_{s,r}b^{h'} \equiv b_{x,y}b^h \pmod{p^k}$. This implies that g is well-defined.

Assume that $g(\bar{a}_{s,r}\bar{a}^h) = g\left(\bar{a}_{x,y}\bar{a}^{h'}\right)$, where $h, h' \in \mathbb{N}$, $s, x \in \{0,1,2,\dots,k-1\}, r \in \{1,2,3,\dots,n_s\}$ and $y \in \{1,2,3,\dots,n_x\}$. Therefore, we have $\bar{b}_{s,r}\bar{b}^h = \bar{b}_{x,y}\bar{b}^{h'}$. Since $\bar{b}_{s,r}\bar{b}^h \in V(P'_{s,r})$ and $\bar{b}_{x,y}\bar{b}^{h'} \in V(P'_{x,y})$, we have $P'_{s,r} = P'_{x,y}$, which implies that $s = x$ and $r = y$. Thus, $\bar{b}_{s,r} = \bar{b}_{x,y}$ and $\bar{a}_{s,r} = \bar{a}_{x,y}$. Since $b_{s,r}b^h \equiv b_{s,r}b^{h'} \pmod{p^k}$ and $gcd(b_{s,r}, p^k) = p^s$, we have $b^h \equiv b^{h'} \pmod{p^{k-s}}$. We assume that $h < h'$ then we have $1 \equiv b^{h'-h} \pmod{p^{k-s}}$. This implies that $m|(h'-h)$, where $ord_{p^{k-s}}a = m = ord_{p^{k-s}}b$. Then there exists $c \in \mathbb{N}$ such that $mc + h = h'$. We then have $a^{h'} = a^{mc}a^h \equiv a^h \pmod{p^{k-s}}$. From $\gcd(a_{s,r}, p^k) = p^s$ and $\bar{a}_{s,r} = \bar{a}_{x,y}$, we obtain that $a_{s,r}a^{h'} \equiv a_{x,y}a^h \pmod{p^k}$. It is easy to show that g is surjective. From the definition of g and it's injectivity, we conclude that g is an isomorphism.

Example 10. Consider $Cay(\mathbb{Z}_{16}, \bar{3})$ and $Cay(\mathbb{Z}_{16}, \overline{11})$. From $ord_{2^4}3 = 4 = ord_{2^4}11$, $ord_{2^{4-1}}3 = 2 = ord_{2^3}11$, $ord_{2^{4-2}}3 = 2 = ord_{2^2}11$, $ord_{2^{4-3}}3 = 1 = ord_2 11$ and Theorem 9, we then have $Cay(\mathbb{Z}_{16}, \bar{3})$ is isomorphic to $Cay(\mathbb{Z}_{16}, \overline{11})$.

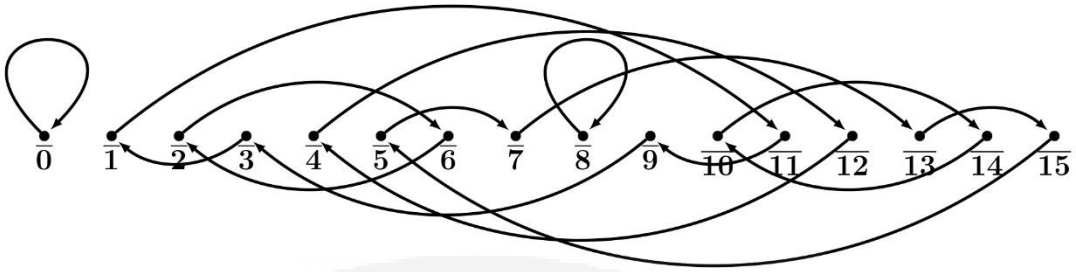

Figure 4 $Cay(\mathbb{Z}_{16}, \overline{11})$

References

Hosseinzadeh, N., & Assari, A. (2014). Graph operations on Cayley graph of semigroup. *International Journal of Applied Mathematical Research*, *3*(1), 54-57.

Kelarev, A., & Praeger, C. (2003). On transitive Cayley graphs of groups and semigroups. *European Journal of Combinatorics*, *24*, 59-72.

Khosravi, B. (2016). Some properties of Cayley graphs of cancellative semigroups. *Proceeding of the Romanian academy, Series A*, *14*, 3-10.

Konstantinova, E. (2008). Some problems on Cayley graphs. *Linear Algebra and its applications*, *429*, 2754-2755.

Suksumran, T., & Panma, S. (2015). On connected Cayley graphs of semigroups. *Thai Journal of Mathematics*, *13*, 541-652.