DIRECTED GRAPHS OF FINITE RINGS

A PREPRINT

Paige Beyer

Mathematics and Statistics Department

Dordt University

Sioux Center IA 51250

pgbyr@dordt.edu

Hannah Fields

Mathematics and Statistics Department

Dordt University

Sioux Center IA 51250

hnnhflds@dordt.edu

July 23, 2019

ABSTRACT

The directed graph of a ring is a graphical representation of its additive and multiplicative structure. Using the following relationship $(a, b) \to (a + b, ab)$, we can construct a unique directed graph for every ring. In this paper, we will focus on the incoming degrees of vertices in the directed graphs of finite rings with distinct specifications.

Acknowledgements: We would like to thank the Dordt University Office of Research and Scholarship for making this research possible. We would also like to thank Dr. Mike Janssen and Dr. Melissa Lindsey for their guidance throughout.

1 Introduction

Different manifestations of graph theory have been produced over time to acquire information regarding ring theory, including zero-divisor graphs, commuting graphs, and directed graphs. Cayley tables are used to give us a straightforward visual representation of the structure of rings. But since rings have both additive and multiplicative structures, it takes two Cayley tables to fully represent a ring. We turn to directed graphs to give a single representation of a ring while maintaining the desired structure.

Directed graphs were first proposed by Lipkovski in [9]. The knowledge and use of directed graphs have been expanded through the work of Hausken and Skinner in [5] as well as Ang and Shulte in [1]. The results of Hausken and Skinner helped us determine the general structure of directed graphs of commutative rings. Ang and Shulte provided us with information about the possible incoming degrees of vertices in the directed graphs of integral domains.

This paper is a continuation of the work done by the pairs Hausken and Skinner and Ang and Shulte. We will be employing the same conventions and notations used in their papers, and reproducing their results when necessary. The focus of this paper is on the incoming degrees of vertices in $\Psi(\mathbb{Z}_n)$. Special emphasis is placed on the incoming degrees of vertices in $\Psi(\mathbb{Z}_{p^2})$ and $\Psi(\mathbb{Z}_{p^3})$.

In Section 2, the necessary background will be given to understand the paper. The conjectures in Section 3 will be beneficial in grasping the general ideas we look at throughout the paper. Section 4 will explore the varying incoming degrees of vertices in $\Psi(\mathbb{Z}_{p^2})$ as well as why these differences exist. Similarly, Section 5 will look at the different incoming degrees of vertices in $\Psi(\mathbb{Z}_{p^3})$. We will briefly cover the incoming degrees of vertices in $\Psi(\mathbb{Z}_{2p})$ in Section 6. Finally, Section 7 will give additional ideas for future research.

2 Background

This paper contains concepts from both ring theory and graph theory. We will begin by defining some basic concepts needed for this paper, and further define concepts as they become relevant. For further explanation of ring theory, see [2], [4], [6], [8]. For further explanation of graph theory, see [3].

The following definitions are from ring theory, many of which are reproduced from [7].

Definition 1. A *ring* R is a nonempty set, together with binary operations addition (+) and multiplication ($\cdot$) satisfying the following axioms.

R1. Given any $a, b, c \in R$, $(a + b) + c = a + (b + c)$.

R2. Given any $a, b \in R, a + b = b + a$.

R3. There exists an element $0_R \in R$ such that for all $a \in R, a + 0_R = 0_R + a = a$.

R4. Given any $a \in R$ there exists a $b \in R$ such that $a + b = b + a = 0_R$.

R5. Given any $a, b, c \in R, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

R6. For all $a, b, c \in R, a \cdot (b + c) = a \cdot b + a \cdot c$.

R7. For all $a, b, c \in R, (a + b) \cdot c = a \cdot c + b \cdot c$.

A given ring R is called *commutative* if multiplication in the ring is commutative. That is, for all $a, b \in R$, $ab = ba$. A given ring R is said to have *identity* if there exists $1 \in R$ such that $a \cdot 1 = a$ for all $a \in R$. By a *ring*, we generally mean a commutative ring with identity, denoted R, unless otherwise specified.

Definition 2. A *zero divisor* is an element a of a commutative ring R such that there is a nonzero element $b \in R$ such that $ab = ba = 0_R$.

Note that this implies that 0 is a zero-divisor in every non-trivial ring.

Definition 3. The *modulo* operation of two positive numbers a and n, abbreviated a mod n, is the remainder of the Euclidean division of a by n, where a is the dividend and n is the divisor.

For example, 7 mod $3 = 1$ because 7 divided by 3 has a quotient of 2 and a remainder of 1. The result of the modulo operation is an equivalence class, and we will represent this using the least positive residue (i.e. the remainder of the Euclidean division). Then since $7 \equiv 1$ mod 3, the least positive residue is denoted as $7 = \bar{1}$.

Everything that follows will use the notation of the least positive residue unless otherwise specified.

Definition 4. The $\mathbb{Z}_n$ *ring* is the partition of $\mathbb{Z}$ in which the elements are related by the congruence module n.

Definition 5. A *Cayley table* for $\mathbb{Z}_n$ is an addition or multiplication table that arranges the $n \times n$ possible sums/products mod n of the elements in $\mathbb{Z}_n$.

The following definitions from graph theory help us understand the general structure of a directed graph.

Definition 6. For a *graph G*, the set of vertices is denoted $V(G)$ and the set of edges is denoted $E(G)$. An edge (x, y) joins vertices x and y.

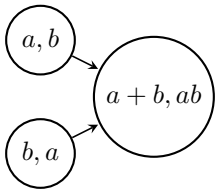
Definition 7. A *directed edge* is an ordered pair of vertices, which we will denote as $x \to y$, for $x, y \in V(G)$. We will also say that x points to y meaning there exists a directed edge $x \to y$.

Definition 8. A *directed graph*, or *digraph*, is a graph where all edges are directed edges.

Definition 9. The digraph of R, denoted $\Psi(R)$, is the graph with $V(\Psi(R)) = R \times R$. For distinct $(a, b), (c, d) \in R \times R$, $(a, b) \to (c, d)$ if and only if $a + b = c$ and $a \cdot b = d$. Because R is commutative, $(b, a) \to (c, d)$ as well.

Figure 1 is a general example of a directed graph.

Figure 1: General Directed Graph

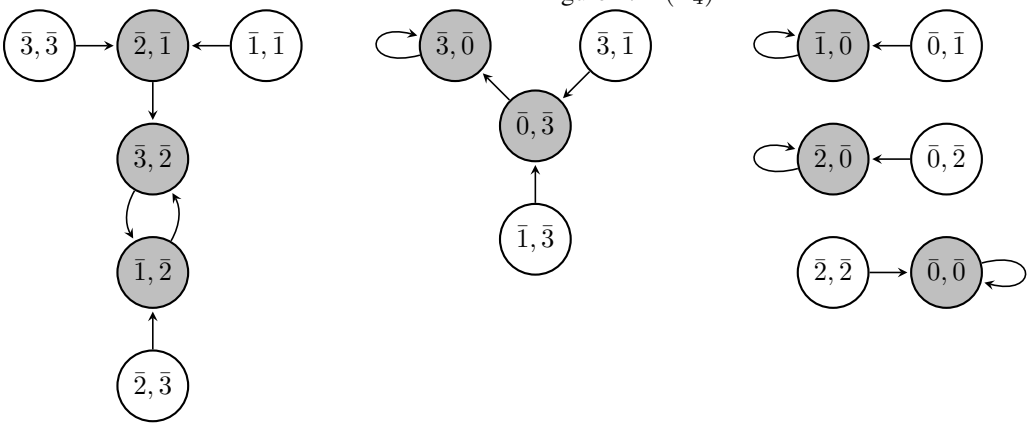


Definition 10. A vertex in $\Psi(R)$ has *incoming degree* n if there are n distinct vertices pointing to it.

Definition 11. A *source* is a vertex with incoming degree zero. The set of all sources in the digraph of a ring is denoted $\mathcal{S}(\Psi(R))$.

Figure 2 is an example of the directed graph of $\mathbb{Z}_4$*. Note that all arithmetic is done modulo* 4*. The shaded vertices have incoming degree 2, while all other vertices are sources.*

Figure 2: $\Psi(\mathbb{Z}_4)$



3 Conjectures

Conjecture 1. *Let* $\Psi(\mathbb{Z}_{p^2})$ *be the digraph of the ring* $\mathbb{Z}_{p^2}$ *where* p *is an odd prime. Then the highest incoming degree of any vertex in* $\Psi(\mathbb{Z}_{p^2})$ *is* p *and the following hold.*

1. $\exists\, p^2$ *vertices with incoming degree* p

2. *We will write each vertex in the form* (x, y)

3. $\{(x, y) \in \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} |$ *when* $x \in \mathbb{Z}_{p^2}$ *is even,* $y = (\frac{x}{2})^2\}$

4. $\{(x, y) \in \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} |$ *when* $x \in \mathbb{Z}_{p^2}$ *is odd,* $y = (\frac{p^2+x}{2})^2\}$

Conjecture 2. *Let* $\Psi(\mathbb{Z}_{p^3})$ *be the digraph of the ring* $\mathbb{Z}_{p^3}$ *where* p *is an odd prime. Then there are* $\frac{p-1}{2} \cdot p^3$ *vertices with the highest incoming degree* $2p$*. Also there are* p^3 *vertices of the form* $(\overline{2a}, \overline{a^2})$ *with incoming degree* p*.*

Conjecture 3. *Let* $\Psi(\mathbb{Z}_{2p})$ *be the digraph of* $\mathbb{Z}_{2p}$ *where* p *is an odd prime. This digraph has incoming degrees of 0, 1, 2, and 4.*

4 Digraphs of $\mathbb{Z}_{p^2}$

Lemma 1. *Let D be the set of zero divisors in $\mathbb{Z}_{p^2}$ where p is an odd prime. Then $D = \{\overline{0}, \overline{p}, \overline{2p}, \ldots, \overline{(p-1)p}\}$. Observe $|D| = p$. Thus for every $\bar{x}, \bar{y} \in D$, $\overline{xy} = \bar{0}$.*

Proof. Let $\bar{a}$ be a nonzero element in $\mathbb{Z}_{p^2}$. Then some nonzero $\bar{b} \in \mathbb{Z}_{p^2}$ is a zero divisor if $\overline{ab} = \bar{0}$. This can only be true if $\overline{p^2}|\overline{ab}$. Since $\bar{a}, \bar{b} < \overline{p^2}$ and $\bar{p}$ is prime, $\bar{a}$ and $\bar{b}$ must both be multiples of $\bar{p}$. □

The following theorems help us determine the possible incoming degrees of vertices in $\mathbb{Z}_{p^2}$.

Theorem 1. *Let $\Psi(\mathbb{Z}_{p^2})$ be the digraph of $\mathbb{Z}_{p^2}$ where p is an odd prime. Then for all $\bar{a} \in \mathbb{Z}_{p^2}$ the vertices of the form $(\overline{2a}, \overline{a^2})$ have incoming degree p.*

Proof. Note that all arithmetic following is done modulo p^2.

Let $S_a = \{(\bar{x}, \bar{y}) \in \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} | (\bar{x}, \bar{y}) \to (\overline{2a}, \overline{a^2})\}$. Let $E = \{0, 1, 2, \ldots, p-1\}$. Observe $|E| = p$.

Consider $(\overline{a+pk}, \overline{a-pk}) \in \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ where $k \in E$. We can show that $(\overline{a+pk}, \overline{a-pk}) \in S_a$. Observe:

$$\begin{aligned}(\overline{a+pk}) + (\overline{a-pk}) &= \bar{a} + \bar{a} \\ &= \overline{2a}\end{aligned}$$

and

$$\begin{aligned}(\overline{a+pk})(\overline{a-pk}) &= \overline{a^2} - \overline{apk} + \overline{apk} - \overline{(pk)^2} \\ &= \overline{a^2} - \overline{(pk)^2}\end{aligned}$$

Since $\overline{(pk)^2} = \bar{0}$ by Lemma 1, $(\overline{a+pk})(\overline{a-pk}) = \overline{a^2}$. Thus $(\overline{a+pk}, \overline{a-pk}) \to (\overline{2a}, \overline{a^2})$ for all $k \in E$. Suppose there exist distinct elements $k_1, k_2 \in E$ such that $\overline{(a+pk_1)} = \overline{(a+pk_2)}$. Without loss of generality assume $k_1 > k_2$. Then

$$\begin{aligned}\overline{pk_1} &= \overline{pk_2} \\ \bar{p}(\overline{k_1 - k_2}) &= \bar{0}\end{aligned}$$

So either $\overline{k_1 - k_2} = \bar{0}$ or $p|\overline{k_1 - k_2}$. But $k_2 < k_1 < p$. Thus $k_1 = k_2$. So for each k_i, $\overline{a+pk_i}$ is distinct. Thus there are exactly p distinct elements of the form $\overline{a+pk} \in \mathbb{Z}_{p^2}$, so there are at least p distinct vertices that point to $(\overline{2a}, \overline{a^2})$.

Now suppose there are other vertices in S_a not of the form $(\overline{a+pk}, \overline{a-pk})$. Let $\bar{x} \in \mathbb{Z}_{p^2}$. We can use the

Division Algorithm to say that $x - a = pk + r$ where $0 \leq r < p$. Since $0 \leq x, a < p^2$, $-p^2 < x - a < p^2$. So $\overline{x-a} \in \{\bar{0}, \bar{1}, \ldots, \overline{p^2-1}\}$. Then $\overline{x-a} = \bar{p}\bar{k} + \bar{r}$. Because $\overline{x-a} < \overline{p^2}$, $\bar{k} < \bar{p}$. So we can write any $\bar{x} \in \mathbb{Z}_{p^2}$ as $\overline{a+pk+r}$. We have already covered the case where $r = 0$. Now assume $0 < r < p$ and $(\overline{a+pk+r}, \overline{a-pk-r}) \to (\overline{2a}, \overline{a^2})$. Then

$$\begin{aligned}(\overline{a+pk+r}) + (\overline{a-pk-r}) &= \bar{a} + \bar{a} \\ &= \overline{2a}\end{aligned}$$

and

$$\begin{aligned}(\overline{a+pk+r})(\overline{a-pk-r}) &= \overline{a^2} - \overline{apk} - \overline{ar} + \overline{apk} - \overline{(pk)^2} - \overline{pkr} + \overline{ar} - \overline{pkr} - \overline{r^2} \\ &= \overline{a^2} - \overline{2pkr} - \overline{(pk)^2} - \overline{r^2} \\ &= \overline{a^2} - \overline{2pkr} - \overline{r^2} \qquad \text{(recall } \overline{(pk)^2} = \bar{0}\text{)} \\ &= \overline{a^2} - \overline{r}(\overline{2pk-r})\end{aligned}$$

Let D be as in Lemma 1. Since $0 < \bar{r} < p$, $\bar{r} \notin D$. Then $(\overline{a+pk+r})(\overline{a-pk-r}) = \overline{a^2}$ only if $(\overline{2pk-r}) = \bar{0}$. Let's assume $(\overline{2pk-r}) = \bar{0}$. Then $(\overline{2pk}) = \bar{r}$. But $\bar{r}$ is not a multiple of p. Thus $(\overline{a+pk+r})(\overline{a-pk-r}) \neq \overline{a^2}$. So only vertices of the form $(\overline{a+pk})$ point to $(\overline{2a}, \overline{a^2})$. Therefore all vertices of the form $(\overline{2a}, \overline{a^2}) \in \Psi(\mathbb{Z}_{p^2})$ have incoming degree p. □

Theorem 2. *Let $\Psi(\mathbb{Z}_{p^2})$ be the digraph of $\mathbb{Z}_{p^2}$ where p is an odd prime. Then for $\bar{a} \in \mathbb{Z}_{p^2}$ all non-source vertices not of the form $(\overline{2a}, \overline{a^2})$ have incoming degree 2.*

Proof. Suppose $(\bar{c}, \bar{d})$ is a vertex in $\Psi(\mathbb{Z}_{p^2})$ which is not of the form $(\overline{2a}, \overline{a^2})$ and is not a source. Then $(\bar{c}, \bar{d}) = (\overline{e+f}, \overline{ef})$ for some $\bar{e}, \bar{f} \in \mathbb{Z}_{p^2}$ with $\bar{e} \neq \bar{f}$. Then the vertices $(\bar{e}, \bar{f})$ and $(\bar{f}, \bar{e})$ both point to $(\bar{c}, \bar{d})$, thus the incoming degree of $(\bar{c}, \bar{d})$ is at least 2.

Now suppose there exists a vertex $(\bar{g}, \bar{h}) \in \Psi(\mathbb{Z}_{p^2})$ such that $(\bar{g}, \bar{h}) \notin \{(\bar{e}, \bar{f}), (\bar{f}, \bar{e})\}$ and $(\bar{g}, \bar{h}) \to (\bar{c}, \bar{d})$. If $\bar{g} = \bar{e}$, then $(\bar{g}, \bar{h}) = (\bar{e}, \bar{f})$ and $(\bar{h}, \bar{g}) = (\bar{f}, \bar{e})$, and thus the vertices $(\bar{g}, \bar{h})$ and $(\bar{h}, \bar{g})$ are not distinct from $(\bar{e}, \bar{f})$ and $(\bar{f}, \bar{e})$. The same is true when $\bar{g} = \bar{f}, \bar{h} = \bar{e}$, or $\bar{h} = \bar{f}$.

Thus $\bar{e}, \bar{f}, \bar{g}, \bar{h}$ are all distinct in $\mathbb{Z}_{p^2}$. Then

$$\overline{e+f} = \bar{c} = \overline{g+h} \tag{1}$$

$$\overline{ef} = \bar{d} = \overline{gh} \tag{2}$$

Observe:

$$\begin{aligned}
\overline{(e+f)^2} &= \overline{(g+h)^2} \\
\overline{e^2} + \overline{2ef} + \overline{f^2} &= \overline{g^2} + \overline{2gh} + \overline{h^2} \\
\overline{e^2} + \overline{2ef} + \overline{f^2} &= \overline{g^2} + \overline{2ef} + \overline{h^2} && \text{using (2)} \\
\overline{e^2} + \overline{f^2} &= \overline{g^2} + \overline{h^2} \\
\overline{e^2} - \overline{g^2} &= \overline{h^2} - \overline{f^2} \\
\overline{(e+g)(e-g)} &= \overline{(h+f)(h-f)} \\
\overline{(e+g)(h-f)} &= \overline{(h+f)(h-f)} && \text{using (1)} \\
\overline{(h-f)}(\overline{(e+g)} - \overline{(h+f)}) &= \overline{0}
\end{aligned}$$

As noted above, $\bar{h} \neq \bar{f}$. Then since $(\overline{h-f}) \neq \bar{0}$ and $\mathbb{Z}_{p^2}$ contains zero divisors, there are two cases we must consider. Within these case we are aiming for one of two types of contradictions. Either the elements of the vertices are not distinct such that $\bar{g} = \bar{e}, \bar{g} = \bar{f}, \bar{h} = \bar{e}$, or $\bar{h} = \bar{f}$, or one of the vertices $(\bar{e}, \bar{f})$ or $(\bar{g}, \bar{h})$ point to $(\overline{2a}, \overline{a^2})$.

Case 1: $\overline{(e+g)} - \overline{(h+f)} = \bar{0}$.

Observe:

$$\begin{aligned}
\overline{(e+g)} &= \overline{(h+f)} \\
\overline{2e} + \overline{g} + \overline{f} &= \overline{2h} + \overline{g} + \overline{f} && \text{using (1)} \\
\overline{2e} &= \overline{2h}
\end{aligned}$$

Because 2 is not a zero divisor in $\mathbb{Z}_{p^2}$, $\bar{e} = \bar{h}$ which is a contradiction.

Case 2: $\overline{(e+g)} - \overline{(h+f)} \neq \bar{0}$. Thus $\overline{(h-f)}$ is a non-zero zero divisor.

Observe:

$$\overline{(h-f)(g+h)} = \overline{(h-f)(e+f)} \quad \text{using (1)}$$

$$\overline{(h-f)(g+h)} = \overline{(e-g)(e+f)}$$

$$\overline{hg} - \overline{fg} - \overline{fh} + \overline{h^2} = \overline{e^2} - \overline{ge} - \overline{gf} + \overline{ef}$$

$$\overline{h^2} - \overline{fh} = \overline{e^2} - \overline{ge}$$

$$\overline{h(h-f)} = \overline{e(e-g)}$$

Since $(\overline{h-f}) = (\overline{e-g})$ by (1), either $\bar{h}$ is a zero divisor or $\bar{h} = \bar{0}$.

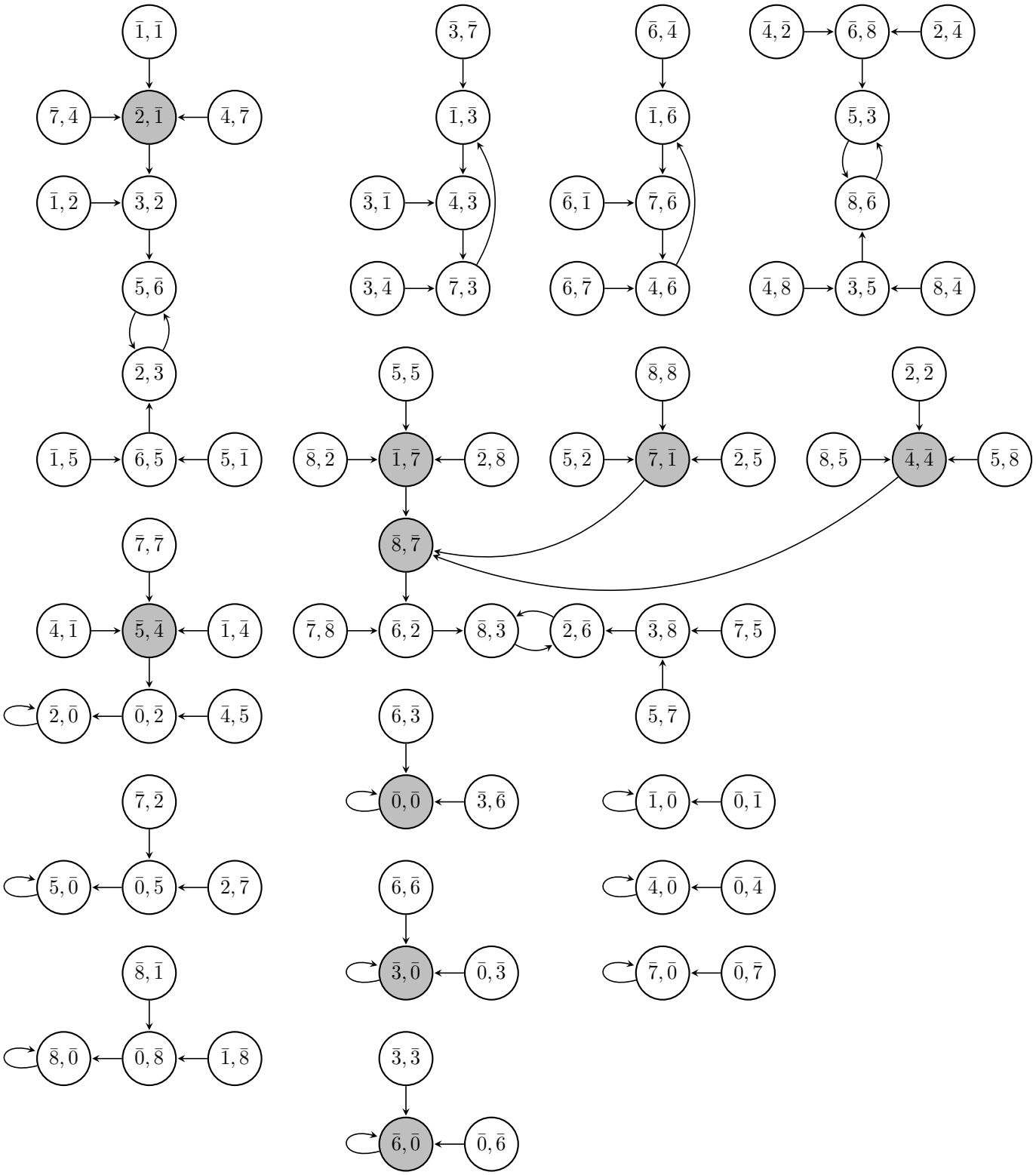
Subcase 2.1: $\bar{h}$ is a zero divisor. Then by rearranging the above line: $\overline{e^2} + \overline{f^2} = \overline{g^2} + \overline{h^2}$ so that $\overline{f^2} - \overline{h^2} = \overline{g^2} - \overline{e^2}$ we can use a similar argument to show that $\bar{g}$ is also a zero divisor. In our proof of Theorem 1 we said that all vertices of the form $(\overline{a+pk}, \overline{a-pk})$ point to $(\overline{2a}, \overline{a^2})$. Thus when $\bar{a}$ is a zero divisor, both elements of the vertex pointing to $(\overline{2a}, \overline{a^2})$ will be any pair of zero divisors. So if $\bar{g}$ and $\bar{h}$ are both zero divisors, they would have to point to something of the form $(\overline{2a}, \overline{a^2})$ which is a contradiction. Thus $(\overline{h-f})$ is not a zero divisor, so $\bar{h} = \bar{f}$ which is a contradiction.

Subcase 2.2: $\bar{h} = \bar{0}$. Then $\bar{e}$ and $(\overline{e-g})$ are zero divisors as $\bar{h} \neq \bar{e}$. Then $\bar{g}$ must also be a zero divisor. Using the above equation $\overline{(h-f)(g+h)} = \overline{(h-f)(e+f)}$, we can replace the left $(\overline{h-f})$ with $(\overline{e-g})$ so that $\overline{(e-g)(g+h)} = \overline{(h-f)(e+f)}$. Using a similar argument as above, we can show that $\bar{g}(\overline{e-g}) = \bar{f}(\overline{h-f})$. Then $\bar{f}$ is also a zero divisor, and thus from our proof of Theorem 1 $(\bar{e}, \bar{f})$ points to a vertex of the form $(\overline{2a}, \overline{a^2})$. Thus $\bar{h} \neq \bar{0}$ which is a contradiction.

Therefore all non-source vertices in $\Psi(\mathbb{Z}_{p^2})$ not of the form $(\overline{2a}, \overline{a^2})$ have incoming degree 2. □

Figure 3 is the directed graph of $\mathbb{Z}_9$, an example of $\Psi(\mathbb{Z}_{p^2})$. Note that all arithmetic is done modulo 9. The shaded vertices have incoming degree 3, while all other non-source vertices having incoming degree 2.

Figure 3: $\Psi(\mathbb{Z}_9)$



Corollary 1. *The maximum incoming degree in $\Psi(\mathbb{Z}_{p^2})$ is p.*

Theorem 3. *Let $\mathcal{S}(\Psi(\mathbb{Z}_{p^2}))$ be the set of sources in $\mathbb{Z}_{p^2}$ where $|V(\Psi(\mathbb{Z}_{p^2}))| = p^4$. Then $|\mathcal{S}(\Psi(\mathbb{Z}_{p^2}))| = \frac{p^4+p^3-2p^2}{2}$.*

Proof. All vertices in $\Psi(\mathbb{Z}_{p^2})$ which are not sources will be of the form $(\overline{2a}, \overline{a^2})$ or $(\overline{c+d}, \overline{cd})$ for distinct $\bar{c}, \bar{d} \in \mathbb{Z}_{p^2}$ such that $(\bar{c}, \bar{d}) \not\to (\overline{2a}, \overline{a^2})$. Counting the number of vertices of these two forms will yield the desired result.

For every $\bar{a} \in \mathbb{Z}_{p^2}$, $(\bar{a}, \bar{a}) \to (\overline{2a}, \overline{a^2})$. So the number of vertices of the form $(\overline{2a}, \overline{a^2})$ is p^2. By Theorem 1, there are p vertices that point to $(\overline{2a}, \overline{a^2})$, then there is a total of $p \cdot p^2$ vertices that point to vertices of the form $(\overline{2a}, \overline{a^2})$. Since there are p^4 vertices in $\Psi(\mathbb{Z}_{p^2})$, then $p^4 - p^3$ of the vertices are of the form $(\bar{c}, \bar{d})$ or $(\bar{d}, \bar{c})$. By Theorem 2, non-source vertices in $\Psi(\mathbb{Z}_{p^2})$ not of the form $(\overline{2a}, \overline{a^2})$ have incoming degree 2. Then since exactly two vertices point to each vertex of the form $(\overline{c+d}, \overline{cd})$, there are $\frac{p^4-p^3}{2}$ vertices of the form $(\overline{c+d}, \overline{cd})$.

Thus there are $p^2 + \frac{p^4-p^3}{2} = \frac{p^4-p^3+2p^2}{2}$ vertices in $\Psi(\mathbb{Z}_{p^2})$ that are not sources. Therefore there are $p^4 - \frac{p^4-p^3+2p^2}{2} = \frac{p^4+p^3-2p^2}{2}$ vertices which are sources. □

5 Digraphs of $\mathbb{Z}_{p^3}$

Lemma 2. *Let D be the set of zero divisors in $\mathbb{Z}_{p^n}$ where p is an odd prime and $n \geq 2$ for $n \in N$. Then $D = \{0, p, 2p, \ldots, (p^{n-1}-1)p\}$.*

Proof. Let $\bar{a}, \bar{b} \in \mathbb{Z}_{p^n}$ such that $\overline{ab} = \bar{0}$. Then $\overline{p^n} | \overline{ab}$. Since p is prime, $\bar{a}$ and $\bar{b}$ must both be multiples of p, so $\bar{a}, \bar{b} \in D$. □

The following theorems determine the incoming degree of certain types of vertices in $\mathbb{Z}_{p^3}$.

Theorem 4. *Let $\Psi(\mathbb{Z}_{p^3})$ be the digraph of $\mathbb{Z}_{p^3}$ where p is an odd prime. Then for all $\bar{a} \in \mathbb{Z}_{p^3}$ the vertices of the form $(\overline{2a}, \overline{a^2})$ have incoming degree p.*

Proof. Note that all arithmetic following is done modulo p^3.

Let $S_a = \{(\bar{x}, \bar{y}) \in \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3} | (\bar{x}, \bar{y}) \to (\overline{2a}, \overline{a^2})\}$. Let $E = \{0, 1, 2, \ldots, p-1\}$. Observe $|E| = p$.

Consider $(\overline{a+p^2k}, \overline{a-p^2k}) \in \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3}$ where $k \in E$. We can show that $(\overline{a+p^2k}, \overline{a-p^2k}) \in S_a$.

Observe:

$$(\overline{a+p^2k}) + (\overline{a-p^2k}) = \bar{a} + \bar{a}$$

$$= \overline{2a}$$

and

$$\begin{aligned}(\overline{a+p^2k})(\overline{a-p^2k}) &= \overline{a^2} - \overline{ap^2k} + \overline{ap^2k} - \overline{(p^2k)^2} \\ &= \overline{a^2} - \overline{(p^2k)^2}\end{aligned}$$

Since $\overline{(p^2k)^2} = \bar{0}$, $(\overline{a+p^2k})(\overline{a-p^2k}) = \overline{a^2}$. Thus $(\overline{a+p^2k}, \overline{a-p^2k}) \to (\overline{2a}, \overline{a^2})$ for all $k \in E$. Suppose there exist distinct elements $k_1, k_2 \in E$ such that $\overline{(a+p^2k_1)} = \overline{(a+p^2k_2)}$. Without loss of generality assume $k_1 > k_2$. Then

$$\overline{p^2k_1} = \overline{p^2k_2}$$

$$\overline{p^2}(\overline{k_1 - k_2}) = \bar{0}$$

So either $\overline{k_1 - k_2} = \bar{0}$ or $\overline{p^2} | \overline{k_1 - k_2}$. But $0 \leq k_2 < k_1 < p$, so $\overline{p^2} \nmid \overline{k_1 - k_2}$. Thus $k_1 = k_2$. So for each $k_i \in E$, $\overline{a+p^2k_i}$ is distinct. Since there are exactly p distinct elements of the form $\overline{a+p^2k} \in \mathbb{Z}_{p^3}$, there are at least p distinct vertices that point to $(\overline{2a}, \overline{a^2})$.

Now suppose there are other vertices in S_a not of the form $(\overline{a+p^2k}, \overline{a-p^2k})$. Let $\bar{x} \in \mathbb{Z}_{p^3}$. We can use the Division Algorithm to say that $x - a = p^2k + r$ where $0 \leq r < p^2$. Since $0 \leq x, a < p^3$, $-p^3 < x - a < p^3$. So $\overline{x-a} \in \{\bar{0}, \bar{1}, \ldots, \overline{p^3 - 1}\}$. Then $\overline{x-a} = \overline{p^2}\bar{k} + \bar{r}$. Because $\overline{x-a} < \overline{p^3}$, $\bar{k} < \bar{p}$. So we can write any $\bar{x} \in \mathbb{Z}_{p^3}$ as $\overline{a+p^2k+r}$. We have already covered the case where $r = 0$. Now assume $0 < r < p^2$ and $(\overline{a+p^2k+r}, \overline{a-p^2k-r}) \to (\overline{2a}, \overline{a^2})$. Then

$$\begin{aligned}(\overline{a+p^2k+r}) + (\overline{a-p^2k-r}) &= \bar{a} + \bar{a} \\ &= \overline{2a}\end{aligned}$$

and

$$\begin{aligned}(\overline{a+p^2k+r})(\overline{a-p^2k-r}) &= \overline{a^2} - \overline{ap^2k} - \overline{ar} + \overline{ap^2k} - \overline{(p^2k)^2} - \overline{p^2kr} + \overline{ar} - \overline{p^2kr} - \overline{r^2} \\ &= \overline{a^2} - \overline{2p^2kr} - \overline{(p^2k)^2} - \overline{r^2} \\ &= \overline{a^2} - \overline{2p^2kr} - \overline{r^2} \qquad \text{(recall } \overline{(p^2k)^2} = \bar{0}\text{)} \\ &= \overline{a^2} - \overline{r}(\overline{2p^2k - r})\end{aligned}$$

So either $\bar{r}$ is a zero divisor or $\overline{2p^2k - r} = \bar{0}$. Suppose $\overline{2p^2k - r} = \bar{0}$. Then $\overline{2p^2k} = \bar{r}$, but $0 < r < p^2$. So $\bar{r}$ is not a multiple of $\overline{p^2}$. Now suppose $\bar{r}$ is a zero divisor. By Lemma 2 $\bar{r}$ is of the form $\overline{pj}$ where $0 < j \leq (p-1)$.

Observe:

$$\begin{aligned}\overline{2p^2kr} - \overline{r^2} &= \overline{2p^2kpj} - \overline{(pj)^2} \\ &= \overline{2p^3kj} - \overline{p^2j^2}\end{aligned}$$

Then $\overline{2p^3kj} = \bar{0}$. But $\overline{p^2j^2} \neq \bar{0}$ because $j < p$. Thus $(\overline{a + p^2k + r})(\overline{a - p^2k - r}) \neq \overline{a^2}$. Therefore all vertices of the form $(\overline{2a}, \overline{a^2}) \in \Psi(\mathbb{Z}_{p^3})$ have incoming degree p. □

Theorem 5. *Let $\Psi(\mathbb{Z}_{p^3})$ be the digraph of $\mathbb{Z}_{p^3}$ where p is an odd prime. Then for all $\bar{a} \in \mathbb{Z}_{p^3}$, vertices of the form $(\overline{2a}, \overline{a^2 - (pk)^2})$ have incoming degree $2p$.*

Proof. Let $T_a = \{(\bar{x}, \bar{y}) \in \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3} | (\bar{x}, \bar{y}) \to (\overline{2a}, \overline{a^2 - (pk)^2})\}$.

Let $E = \{0, 1, \ldots, p^2 - 1\} \setminus \{0, p, 2p, \ldots, (p-1)p\}$. Let $F = \{\overline{pk} | k \in E\}$.

Consider $(\overline{a + pk}, \overline{a - pk}) \in \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3}$ for all $\overline{pk} \in F$. We can show that $(\overline{a + pk}, \overline{a - pk}) \in T_a$.

Observe:

$$\begin{aligned}(\overline{a + pk}) + (\overline{a - pk}) &= \bar{a} + \bar{a} \\ &= \overline{2a}\end{aligned}$$

and

$$\begin{aligned}(\overline{a + pk})(\overline{a - pk}) &= \overline{a^2} - \overline{apk} + \overline{apk} - \overline{(pk)^2} \\ &= \overline{a^2} - \overline{(pk)^2}\end{aligned}$$

Consider k_1, k_2, distinct elements in E such that $\bar{p} | \overline{k_1 + k_2}$.

Observe:

$$\overline{pg} = \overline{k_1 + k_2}$$

$$\overline{pg}(\overline{k_1 - k_2}) = \overline{(k_1)^2 - (k_2)^2}$$

$$\overline{p} | \overline{(k_1)^2 - (k_2)^2}$$

$$\overline{ph} = \overline{(k_1)^2 - (k_2)^2}$$

$$\overline{p^3h} = \overline{p^2(k_1)^2 - p^2(k_2)^2}$$

$$\overline{p^3} | \overline{p^2(k_1)^2 - p^2(k_2)^2}$$

$$\overline{p^2(k_1)^2} = \overline{p^2(k_2)^2}$$

Since $\overline{p^2(k_1)^2} = \overline{p^2(k_2)^2}$, $(\overline{a+pk_1}, \overline{a-pk_1})$ and $(\overline{a+pk_2}, \overline{a-pk_2})$ point to the same vertex. Consider the set of the first $p-1$ elements in E. There are exactly $\frac{p-1}{2}$ distinct pairs of elements k_i and k_j such that $\bar{p}|\overline{k_i+k_j}$. If we then look at the next set of $p-1$ elements in E along with the first set, there are two different pairings of elements such that $\bar{p}|\overline{k_i+k_j}$. Thus there are $2p$ distinct elements in E creating $2p$ distinct vertices of the form $(\overline{a+pk_i}, \overline{a-pk_i})$ that all point to the same vertex. Therefore all vertices of the form $(\overline{2a}, \overline{a^2-(pk)^2})$ have incoming degree of at least $2p$.

Now suppose there are other vertices in T_a not of the form $(\overline{a+pk}, \overline{a-pk})$. Let $\bar{x} \in \mathbb{Z}_{p^3}$. We can use the Division Algorithm to say that $x - a = pk + r$ where $0 \leq r < p$. Since $0 \leq x, a < p^3$, $-p^3 < x - a < p^3$. So $\overline{x-a} \in \{\bar{0}, \bar{1}, \ldots, \overline{p^3-1}\}$. Then $\overline{x-a} = \bar{p}\bar{k} + \bar{r}$. Because $\overline{x-a} < \overline{p^3}$, $\bar{k} < \overline{p^2}$. So we can write any $\bar{x} \in \mathbb{Z}_{p^3}$ as $\overline{a+pk+r}$. We have already covered the case where $r = 0$. Now assume $0 < r < p$ and $(\overline{a+pk+r}, \overline{a-pk-r}) \to (\overline{2a}, \overline{a^2-(pk)^2})$. Then

$$\begin{aligned}(\overline{a+pk+r}) + (\overline{a-pk-r}) &= \bar{a} + \bar{a} \\ &= \overline{2a}\end{aligned}$$

and

$$\begin{aligned}(\overline{a+pk+r})(\overline{a-pk-r}) &= \overline{a^2} - \overline{apk} - \overline{ar} + \overline{apk} - \overline{(pk)^2} - \overline{pkr} + \overline{ar} - \overline{pkr} - \overline{r^2} \\ &= \overline{a^2} - \overline{(pk)^2} - \overline{2pkr} - \overline{r^2} \\ &= \overline{a^2} - \overline{(pk)^2} - \bar{r}(\overline{2pk-r})\end{aligned}$$

So either $\bar{r}$ is a zero divisor or $\overline{2pk-r} = \bar{0}$. Since $0 < r < p$, r cannot be a zero divisor. Now assume $\overline{2pk-r} = \bar{0}$. Then $\overline{2pk} = \bar{r}$, but $\bar{r}$ cannot be a multiple of $\bar{p}$ because $0 < r < p$. Thus $(\overline{a+p^2k+r})(\overline{a-p^2k-r}) \neq \overline{a^2} - \overline{(pk)^2}$. Therefore all vertices of the form $(\overline{2a}, \overline{a^2-(pk)^2})$ have incoming degree $2p$. □

6 Digraphs of $\mathbb{Z}_{2p}$

Lemma 3. *Let G be the set of zero divisors for $\mathbb{Z}_{2p}$ where p is an odd prime. Then $G = \{\bar{0}, \bar{2}, \bar{4}, \ldots, \overline{(2p-2)}\} \cup \{p\}$. Then $\overline{(2k)p} = \bar{0}$ for $k < p$.*

Theorem 6. *Let $\Psi(\mathbb{Z}_{2p})$ be the digraph of $\mathbb{Z}_{2p}$ where p is an odd prime. Then for all $\bar{a} \in \mathbb{Z}_{2p}$, vertices of the form $(\overline{2a}, \overline{a^2})$ have incoming degree 1.*

Proof. Note that all arithmetic following is done modulo $2p$.

It is always the case that $(\bar{a}, \bar{a}) \to (\overline{2a}, \overline{a^2})$, and thus $(\overline{2a}, \overline{a^2})$ has incoming degree of at least 1.

Now suppose $(\bar{b}, \bar{b}) \to (\overline{2a}, \overline{a^2})$. Then $\overline{2a} = \overline{2b}$ and $\overline{a^2} = \overline{b^2}$. Observe:

$$\overline{2a} - \overline{2b} = \bar{0}$$

$$\overline{2}(\overline{a-b}) = \bar{0}$$

and

$$\overline{a^2} - \overline{b^2} = \bar{0}$$

$$(\overline{a+b})(\overline{a-b}) = \bar{0}$$

By Lemma 3 only something of the form $\overline{2kp}$ is equal to $\bar{0}$. So since $\overline{2}(\overline{a-b}) = \overline{0}$, $(\overline{a-b})$ must be a multiple of p. Since $\bar{a}, \bar{b} < 2p$ and $\bar{a} \neq \bar{b}$, $(\overline{a-b}) = \bar{p}$. Because $\bar{p}$ is odd, $\bar{a}$ is odd and $\bar{b}$ is even or vice versa. Then $(\overline{a+b})$ must be odd, so $(\overline{a+b})(\overline{a-b}) \neq \bar{0}$. Thus $(\bar{b}, \bar{b}) \not\to (\overline{2a}, \overline{a^2})$.

Finally suppose $(\bar{c}, \bar{d}) \to (\overline{2a}, \overline{a^2})$ for distinct $\bar{c}, \bar{d} \in \mathbb{Z}_{2p}$. Then $\overline{c+d} = \overline{2a}$ and $\overline{cd} = \overline{a^2}$. Observe:

$$\overline{(c+d)^2} = \overline{(2a)^2}$$

$$\overline{c^2} + \overline{2cd} + \overline{d^2} = \overline{4a^2}$$

$$\overline{c^2} - \overline{2cd} + \overline{d^2} = \overline{0}$$

$$\overline{(c-d)^2} = \overline{0}$$

By Lemma 3 there does not exist an $\overline{x} \in \mathbb{Z}_{2p}$ such that $\overline{x^2} = \overline{0}$. Thus $\overline{(c-d)^2} \neq \overline{0}$, so $(\overline{c}, \overline{d}) \not\to (\overline{2a}, \overline{a^2})$.

Therefore vertices of the form $(\overline{2a}, \overline{a^2})$ have incoming degree 1. □

7 Future Research

Because the properties and structures of directed graphs are relatively new, future research could be driven in a number of different directions. Our research focused on variations of $\Psi(\mathbb{Z}_{p^n})$ and the incoming degrees of their vertices. One path could look into proving the form of possible vertices with incoming degree 2 in $\Psi(\mathbb{Z}_{p^n})$. Further investigations could help generalize our research for the incoming degrees of vertices in $\Psi(\mathbb{Z}_n)$.

Given a finite ring, continued research toward creating an algorithm to find the possible incoming degrees of the vertices in that ring's digraph, along with the number of vertices associated with each incoming degree is another potential avenue to take. One could continue our work by focusing on finding an algorithm that produces the number of sources for each digraph of a finite ring. Steps could also be taken to help generalize the above theorems for all digraphs of finite rings.

References

[1] Ang, C., Shulte, A. (2013). Directed Graphs of Commutative Rings with Identity. *Rose-Hulman Undergrad. Math. J.:* 14(1): 167-188.

[2] Atiyah, M., Macdonald, I. (1969). *Introduction to Commutative Algebra.* Addison-Wesley, Great Britain.

[3] Bollobás, B. (1998). *Modern Graph Theory.* Springer, New York.

[4] Gallian, J.A. (2010). Contemporary Abstract Algebra. Brooks/Cole Cengage Learning.

[5] Hausken, S., Skinner, J. (2013). Directed Graphs of Commutative Rings. *Rose-Hulman Undergrad. Math. J.:* 14(2): 85-100.

[6] Hungerford, T.W. (1989). *Algebra.* Springer-Verlag.

[7] Janssen, M., Lindsey, M., Modern Algebra, *Pre-print*, (2019).

[8] Kaplansky, I. (1974). *Commutative Rings.* Polygonal Publishing House.

[9] Lipkovski, A.T. (2012). Digraphs Associated with Finite Rings. *Publ. Inst. Math. (Beograd) (N.S.)*. 92(106): 35-41.