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

January 30, 2020

ABSTRACT

The directed graph of a ring, first introduced by Lipkovski, is a graphical representation of its additive and multiplicative structure. Using the relationship $(a, b) \to (a + b, ab)$, we can construct a unique directed graph for every ring. This work builds on the work completed by Hausken and Skinner as well as Ang and Shulte on directed graphs of commutative rings. We determine the possible incoming degrees of vertices in the directed graphs of certain classes of finite rings.

Acknowledgements: We would like to thank the Dordt University Kielstra 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

Graph theory has been used to acquire information regarding ring theory, including zero-divisor graphs [5] and directed graphs. Cayley tables are used to give us a straightforward visual representation of the structure of rings. Rings have both additive and multiplicative structures, so 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 its additive and multiplicative structures.

The connection between directed graphs and ring theory was first proposed by Lipkovski in [11]. Hausken and Skinner [6] determined the general structure of directed graphs of commutative rings. Ang and Shulte [1] provided 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 restating their results when necessary. The focus of this paper is on identifying the incoming degrees of vertices in the directed graphs of $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_{p^3}$, which we denote $\Psi(\mathbb{Z}_{p^2})$ and $\Psi(\mathbb{Z}_{p^3})$

In Section 2, the necessary background will be given to understand the paper. Section 3 will explore the varying incoming degrees of vertices in $\Psi(\mathbb{Z}_{p^2})$ as well as why these differences exist. Similarly, Section 4 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 5. Finally, Section 6 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], [8], and [10]. For further explanation of graph theory, see [3].

Our research centers around the concept of an algebraic ring. A *ring* R is a structure with well-defined addition and multiplication operations. By a *ring*, we generally mean a commutative ring with identity, denoted R, unless otherwise specified. Two examples of rings are the set of all real numbers, $\mathbb{R}$, and the set of all rational numbers, $\mathbb{Q}$. An example of a ring that is not a field is the set of all integers, $\mathbb{Z}$. For more on rings, see [10].

The following definitions are from ring theory, many of which are reproduced from [9].

Definition 2.1. A *zero divisor* is an element a of a ring R such that there is a nonzero element $b \in R$ such that $ab = ba = 0$.

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

Definition 2.2. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$ where $n > 1$. Then we say *a is congruent to b modulo n* if $n|(a - b)$. We write this as $a \equiv b \bmod n$.

Example 2.3. Let $a = 7$, $b = 1$, and $n = 3$. Then $7 \equiv 1 \bmod 3$ because $3|(7 - 1)$.

Definition 2.4. Given a positive integer n and integer a, we define the *least non-negative residue* of a modulo n, denoted $a \bmod n$, to be the remainder of the Euclidean division of a by n, where a is the dividend and n is the divisor.

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

Table 1: Addition table of $\mathbb{Z}_9$

$\times$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Table 2: Multiplication table of $\mathbb{Z}_9$

Definition 2.5. An *equivalence class* is the set of integers congruent mod n, and we will represent this using the least non-negative residue (i.e. the remainder of the Euclidean division).

Using Example 2.3, since $7 \equiv 1 \bmod 3$, the least non-negative residue is denoted as $7 = \bar{1}$. Everything that follows will use the notation $\bar{x}$ to represent the least non-negative residue unless otherwise specified.

Theorem 2.6. *The set of equivalence classes mod n, denoted $\mathbb{Z}_n$, is a ring under the operations addition and multiplication modulo n.*

This is a well-known theorem in abstract algebra. For more details, see [7].

Definition 2.7. A *Cayley table* for $\mathbb{Z}_n$ is an addition or multiplication table that arranges the n^2 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 2.8. For a *graph G*, the set of vertices is denoted $V(G)$ and the set of edges is denoted $E(G)$. An edge is a pair of vertices, $\{x, y\}$, that joins vertices x and y. The vertices x and y are not necessarily distinct.

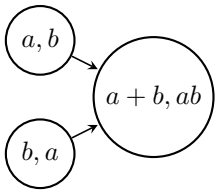

Figure 1: The general structure of a connection in $\Psi(R)$.

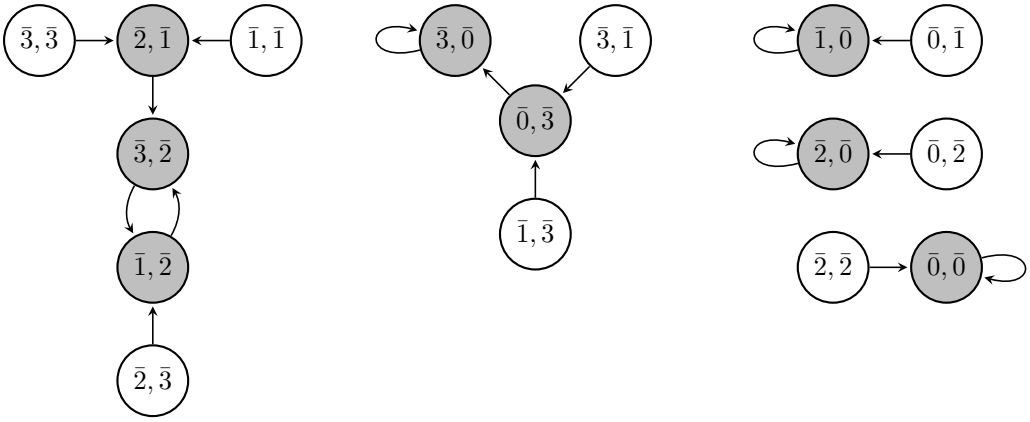

Figure 2: $\Psi(\mathbb{Z}_4)$.

Definition 2.9. 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 2.10. A *directed graph*, or *digraph*, is a graph where all edges are directed edges.

There are many practical applications for directed graphs. Some of these include representing networking problems such as social, railroad, and internet networks. Other uses for digraphs involve family trees and hierarchies as well as predator-prey relationships. For our purposes, they will be used as a way to visually represent finite rings. For more applications of digraphs, see [12].

Definition 2.11. The digraph of some ring R, denoted $\Psi(R)$, is the graph with $V(\Psi(R)) = R \times R$. For $(a, b), (c, d) \in R \times R$, $(a, b) \to (c, d)$ if and only if $a + b = c$ and $a \cdot b = d$. Because R is commutative, $(b, a) \to (c, d)$ when $(a, b) \to (c, d)$.

Definition 2.12. A vertex in $\Psi(R)$ has *incoming degree* n if there are n distinct vertices pointing to it.

Definition 2.13. 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 $\mathbb{Z}_4$. The shaded vertices have incoming degree 2, while all other vertices are sources.

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

In this section, we show that the incoming degrees of vertices in $\Psi(\mathbb{Z}_{p^2})$ are p, 2, or 0. We will also identify the form of vertices that have incoming degree p and the number of sources in each digraph.

Lemma 3.1. *Let D be the set of zero divisors in $\mathbb{Z}_{p^n}$ where p is an odd prime and $n \geq 2$ for $n \in \mathbb{N}$. 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 $p^n | ab$. Since the only factors of p^n are prime, $\bar{a}$ and $\bar{b}$ must both be multiples of p. Thus $\bar{a}, \bar{b} \in D$. □

The following theorems establish the possible incoming degrees of vertices in $\mathbb{Z}_{p^2}$. Note that references to Lemma 3.1 will be specific to when $n = 2$.

Theorem 3.2. *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. To show that all vertices of the form $(\overline{2a}, \overline{a^2})$ have incoming degree p, we will begin by showing that all vertices of the form $(\overline{a + pk}, \overline{a - pk})$ point to vertices of the form $(\overline{2a}, \overline{a^2})$. Then we will show that vertices of any other form do not point to $(\overline{2a}, \overline{a^2})$.

Let $\bar{a} \in \mathbb{Z}_{p^2}$. 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 that $|E| = p$.

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

Observe:

$$(\overline{a + pk}) + (\overline{a - pk}) = \bar{a} + \bar{a} = \overline{2a}$$

and

$$(\overline{a + pk})(\overline{a - pk}) = \overline{a^2} - \overline{apk} + \overline{apk} - \overline{(pk)^2} = \overline{a^2} - \overline{(pk)^2}$$

Since $\overline{(pk)^2} = \bar{0}$ by Lemma 3.1, $(\overline{a + pk})(\overline{a - pk}) = \overline{a^2}$. 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

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

So either $\overline{k_1 - k_2} = \bar{0}$ or $p^2 | p(\overline{k_1 - k_2})$. If $p^2 | p\overline{k_1 - k_2}$, then $p | \overline{k_1 - k_2}$. But $k_2 < k_1 < p$, so $p \not| \overline{k_1 - k_2}$. 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 $\overline{x-a} \in \{0, 1, \ldots, p^2 - 1\}$. 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 $\overline{a+pk+r}$. Since we have already covered the case where $r = 0$, we can 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

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

Let D be as in Lemma 3.1. Since $0 < r < p$, $\bar{r} \notin D$. Then $(\overline{a+pk+r})(\overline{a-pk-r}) = \overline{a^2}$ only if $(\overline{2pk-r}) = \bar{0}$. Assume $(\overline{2pk-r}) = \bar{0}$. Then $(\overline{2pk}) = \bar{r}$. But $\bar{r}$ is not a multiple of $\bar{p}$. 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. □

Now that we have established the existence of p^2 vertices of the form $(\overline{2a}, \overline{a^2})$ that have incoming degree p, and that sources have incoming degree 0 by definition, we consider the non-source vertices not of the form $(\overline{2a}, \overline{a^2})$ in $\Psi(\mathbb{Z}_{p^2})$.

Theorem 3.3. *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. To show that all non-source vertices not of the form $(\overline{2a}, \overline{a^2})$ have incoming degree 2, we will use contradiction to conclude that if $(\bar{e}, \bar{f}) \to (\bar{c}, \bar{d})$ then a vertex (g, h) which is distinct from $(\bar{e}, \bar{f})$ cannot also point to $(\bar{c}, \bar{d})$.

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 $\bar{g} + \bar{f} = \bar{c}$. Since $\bar{g} + \bar{h} = \bar{c}$, $\bar{h} = \bar{f}$. So $(\bar{g}, \bar{h}) = (\bar{e}, \bar{f})$ 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:

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

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 a vertex of the form $(\overline{2a}, \overline{a^2})$.

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: $\overline{(e+g)} - \overline{(h+f)} \neq \bar{0}$, and thus $\overline{(h-f)}$ is a non-zero zero divisor.

Observe:

$$\begin{aligned}
\overline{(h-f)(g+h)} &= \overline{(h-f)(e+f)} && \text{using (1)} \\
\overline{(h-f)(g+h)} &= \overline{(e-g)(e+f)} \\
\overline{hg} - \overline{fg} - \overline{fh} + \overline{h^2} &= \overline{e^2} - \overline{ge} - \overline{gf} + \overline{ef} \\
\overline{h^2} - \overline{fh} &= \overline{e^2} - \overline{ge} \\
\overline{h(h-f)} &= \overline{e(e-g)}
\end{aligned}$$

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

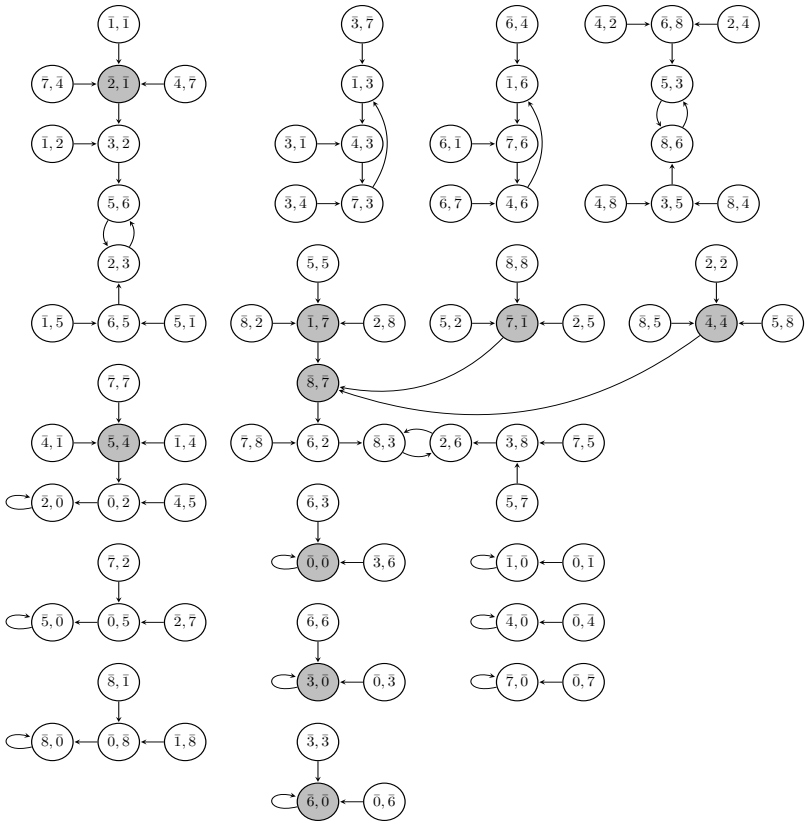

Figure 3: $\Psi(\mathbb{Z}_9)$

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 3.2 we said that all vertices of the form $(\overline{a+pk},\overline{a-pk})$ point to the vertex $(\overline{2a},\overline{a^2})$. 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 3.2 $(\bar{e},\bar{f})$ 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. □

Example 3.4. Figure 3 is the directed graph of $\mathbb{Z}_9$, an example of $\Psi(\mathbb{Z}_{p^2})$. The shaded vertices have incoming degree 3, while all other non-source vertices having incoming degree 2.

Corollary 3.5. *The maximum incoming degree in $\Psi(\mathbb{Z}_{p^2})$ is p.*

Theorem 3.6. *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 3.2, there are p vertices that point to a vertex of the form $(\overline{2a}, \overline{a^2})$, then there is a total of $p \cdot p^2$ vertices that point to all vertices of the form $(\overline{2a}, \overline{a^2})$. Since there are p^4 vertices in $\Psi(\mathbb{Z}_{p^2})$, then there are a total of $p^4 - p^3$ vertices of the form $(\bar{c}, \bar{d})$ where $(\bar{c}, \bar{d}) \not\to (\overline{2a}, \overline{a^2})$. Thus there are $\frac{p^4-p^3}{2}$ vertices of the form $(\overline{c+d}, \overline{cd})$ because by Theorem 3.3, all non-source vertices in $\Psi(\mathbb{Z}_{p^2})$ not of the form $(\overline{2a}, \overline{a^2})$ have incoming degree 2.

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. □

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

This section will identify the form of vertices in $\Psi(\mathbb{Z}_{p^3})$ with incoming degree p or $2p$. Proof techniques will follow similarly to those in Section 3. It is prudent to note that although Lemma 3.1 describes the zero divisors of $\mathbb{Z}_{p^n}$, we will be focusing on when $n = 3$.

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

Theorem 4.1. *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. 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

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

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 $\overline{p^3} | \overline{p^2}(\overline{k_1 - k_2})$. But $0 \leq k_2 < k_1 < p$, so $\overline{p^3} \nmid \overline{p^2}(\overline{k_1 - k_2})$. 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 $x - a < p^3$, $k < p$. 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

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

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 3.1 $\bar{r}$ is of the form $\overline{pj}$ where $j \leq p^{n-1} - 1$.

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. □

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

This section will briefly touch on the form of vertices in $\Psi(\mathbb{Z}_{2p})$ and their incoming degrees, and will follow similar proof techniques to those of Section 3 and 4.

Lemma 5.1. *Let G be the set of zero divisors for $\mathbb{Z}_{2p}$ where p is an odd prime such that $G = \{\bar{0}, \bar{2}, \bar{4}, \ldots, \overline{(2p-2)}\} \cup \{\bar{p}\}$. In particular, if $\bar{x}, \bar{y} \neq \bar{0}$, then $\bar{x}\bar{y} = \bar{0}$ if and only if $2|x$ and $p|y$ or vice versa.*

Proof. Let $\bar{x}, \bar{y} \in G$ be distinct such that $\bar{x}, \bar{y} \neq \bar{0}$ and $\bar{x}\bar{y} = \bar{0}$. Then $2p|\bar{x}\bar{y}$. So $\overline{2pk} = \bar{x}\bar{y}$ where $k < 2p$ for $k \in \mathbb{Z}$. Since p is prime, either $\bar{p}|\bar{y}$ and $2|\bar{x}$ or vice versa.

Now let $2|x$ and $p|y$ or vice versa. Then $\overline{2k} = \bar{x}$ and $\overline{pj} = \bar{y}$ for $k, j \in \mathbb{Z}$. So $\overline{2p(kj)} = \bar{x}\bar{y}$. Thus $\bar{x}\bar{y} = \bar{0}$. □

Theorem 5.2. *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. 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 5.1 only something of the form $\overline{2kp}$ is equal to $\bar{0}$. So since $\overline{2}(\overline{a-b}) = \bar{0}$, $(\overline{a-b})$ must be a multiple of p. Since $a, b < 2p$ 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:

$$\overline{(c+d)^2} = \overline{(2a)^2}$$
$$\overline{c^2} + \overline{2cd} + \overline{d^2} = \overline{4a^2}$$
$$\overline{c^2} - \overline{2cd} + \overline{d^2} = \bar{0}$$
$$\overline{(c-d)^2} = \bar{0}$$

By Lemma 5.1 there does not exist a nonzero $\overline{x} \in \mathbb{Z}_{2p}$ such that $\overline{x^2} = \bar{0}$. Thus $\overline{(c-d)^2} \neq \bar{0}$, so $(\bar{c}, \bar{d}) \not\to (\overline{2a}, \overline{a^2})$.

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

6 Future Research

Because the properties and structures of directed graphs of commutative rings are relatively new, future research could be driven in a number of different directions. While our research focused on specific examples of $\Psi(\mathbb{Z}_{p^n})$, a path for future research could be to generalize our results for $\Psi(\mathbb{Z}_n)$. The following conjecture and questions can be used to help guide this direction of research.

Conjecture 6.1. For a prime p where $p > 2$, vertices in $\Psi(\mathbb{Z}_{2p})$ have incoming degree $0, 1, 2$, or 4.

Question 6.2. Given an arbitrary $n > 1$, what are the possible incoming degrees for vertices in $\Psi(\mathbb{Z}_n)$ (possibly in terms of n)?

Question 6.3. Given a commutative ring R, what ring-theoretic properties are encoded, if any, by the possible incoming degrees in $\Psi(R)$?

Our research led us in several directions. One of those directions looked at the digraphs of primary ideals. The following definitions and conjecture are taken from [6]. We found Conjecture 6.6 to be of interest as it may provide further avenues for exploring Question 6.3. Note that Definition 6.4 has been slightly altered in an attempt to clarify its details. Also recall that for an ideal I of a commutative ring R, the radical of I, written $\sqrt{I}$, is the set $\{r \in R | r^n \in I \text{ for some integer } n > 0\}$.

Definition 6.4. Let Q be a primary ideal of the ring R. The *degree of primality* of Q is the length of the minimal path from a source in $\Psi(\sqrt{Q})$ to any vertex in $\Psi(Q)$.

Definition 6.5. Let Q be a primary ideal of the ring R. The *degree* of Q is the least power n for which every element of $\sqrt{Q}$ is in Q (i.e. $\sqrt{Q}^n = \{r^n | r \in \sqrt{Q}\} \subseteq Q$).

Conjecture 6.6. Let Q be a primary ideal. If the degree of primality of Q is n and the degree of Q is m, then $n + 1 = m$.

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] Guillory, A., Lazo, M., Mondello, L., Naugle, T. (2011). Realizing Zero Divisor Graphs.

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

[7] Hodge, J., Schlicker, S., Sundstrom, T. (2014). *Abstract Algebra an Inquiry-Based Approach* Taylor & Francis Group.

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

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

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

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

[12] Stack Exchange. (2017). Why are Directed Graphs Important. cs.stackexchange.com/questions/68163/why-are-directed-graphs-important.