Rose-Hulman Undergraduate Mathematics Journal

Volume 11
Issue 2

Article 5

Graphs and principal ideals of finite commutative rings

J. Cain
University of Dayton, Dayton OH, cainjoss@notes.udayton.edu

L. Mathewson
Carrol University, Waukesha, WI

A. Wilkens
Beloit College, Beloit, WI

Rose-Hulman Undergraduate Mathematics Journal

Graphs and principal ideals of finite commutative rings

J. Cain[a] L. Mathewson[b] A. Wilkens[c]

Volume 11, no. 2, Fall 2010

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]University of Dayton, Dayton OH
[b]Carroll University, Waukesha, WI
[c]Beloit College, Beloit, WI

Rose-Hulman Undergraduate Mathematics Journal
Volume 11, no. 2, Fall 2010

Graphs and principal ideals of finite commutative rings

J. Cain L. Mathewson A. Wilkens

Abstract. In [1], Afkhami and Khashyarmanesh introduced the cozero-divisor graph of a ring, $\Gamma'(R)$, which examines relationships between principal ideals. We continue investigating the algebraic implications of the graph by developing the reduced cozero-divisor graph, which is a simpler analog.

Acknowledgements: This research was undertaken at the Wabash College Mathematics REU in Crawfordsville, Indiana. It was funded by the National Science Foundation, grant number DMS-0755260. The authors would like to thank Dr. Michael Axtell of the University of St. Thomas, Dr. Joe Stickles of Millikin University, and Wabash College.

1 Introduction

Recent research in commutative algebra has concerned developing a graphical interpretation of the elements of a given ring, and then graph-theoretically analyzing the depiction to reach algebraic conclusions about the ring. The most well-known of these models is the zero-divisor ring, $\Gamma(R)$, first introduced by Anderson and Livingston in [2]. The vertices of $\Gamma(R)$ are precisely the nonzero zero-divisors of the ring R, and two vertices are adjacent if and only if their product is zero. In [1], Afkhami and Khashyarmanesh expanded upon this notion with the cozero-divisor graph, $\Gamma'(R)$, in which the vertices are precisely the nonzero, non-unit elements of R, denoted $W(R)^*$, and two vertices x and y are adjacent if and only if $x \notin (y)$ and $y \notin (x)$; in other words, neither x nor y is a multiple of the other in R. For example, Figure 1 portrays cozero-divisor graph of the ring $\mathbb{Z}_{12}$. They proved several results that demonstrated that $\Gamma(R)$ and $\Gamma'(R)$ are related. For example, for a finite ring R, the vertex sets of the two graphs are equal. (For a discussion on why $\Gamma'(R)$ is called the cozero-divisor graph, see [1].)

In Section 3, we examine some of the results of Afkhami and Khashyarmanesh about $\Gamma'(R)$ and offer additions to some of their theorems. In Section 4, we note that $\Gamma'(R)$ is not the most efficient graph to portray information regarding principal ideals and subset inclusion, and we introduce the reduced cozero-divisor graph, $\Gamma^*(R)$, as a way to improve efficiency. We examine the basic graph-theoretic properties of $\Gamma^*(R)$, as well as its relationship to $\Gamma'(R)$. In Section 5, we explore the algebraic implecations of the structure of $\Gamma^*(R)$. In particular, we examine the ways in which the graph relates to the decomposition of R into a direct product of fields and local rings.

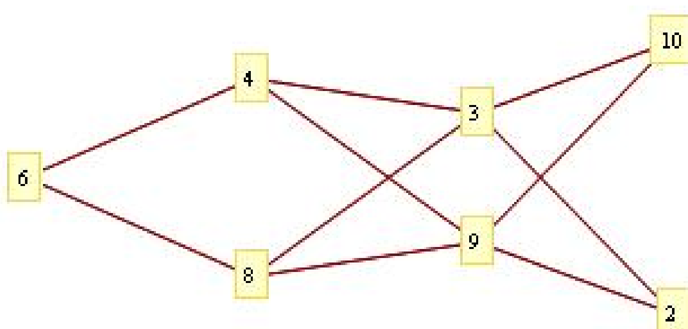

Figure 1: $\Gamma'(\mathbb{Z}_{12})$

2 Background

Let R be a commutative ring with identity and $R^* = R \setminus \{0\}$. Then $r \in R$ is a *zero-divisor* if there exists $z \in R^*$ such that $rz = 0$. The set of zero-divisors of R is denoted $Z(R)$, and the set of nonzero zero-divisors is denoted by $Z(R)^*$. An element a of R is said to be a *unit* of R if there exists a^{-1} such that $aa^{-1} = 1_R$. An *ideal* of R is a subring I of R such that if $a \in I$ and $r \in R$, then $ar \in I$. An ideal M of R is said to be *maximal* if for all ideals

$J \neq M$, $M \subsetneq J$ implies $J = R$. If R has a unique maximal ideal M, R is said to be *local* and is often denoted (R, M).

If $b \in R$, the *principal ideal generated by* b is the ideal $(b) = \{br | r \in R\}$. In general, an ideal is said to be *principal* if it can be generated by an single element of R. The trivial principal ideals of R are $\{0\} = (0)$ and $R = (1) = (u)$ for all units u of R.

A *graph* G is defined as the pair $(V(G), E(G))$, where $V(G)$ is the set of *vertices* of G and $E(G)$ is the set of *edges* of G. An element of $E(G)$ has the form $\{a, b\}$ where $a, b \in V(G)$ and $a \neq b$. If $\{a, b\} \in E(G)$, we say a is *adjacent* to b, and we write a—b. A graph G is said to be *complete* if a—b for all distinct $a, b \in V(G)$, and G is said to be *empty* if $E(G) = \emptyset$. Note by this definition that a graph may be empty even if $V(G) \neq \emptyset$. An empty graph could also be described as *totally disconnected*. If $|V(G)| \geq 2$, a *path* from a to b is a series of adjacent vertices a—v_1—v_2—$\cdots$—v_n—b. The length of a path is the number of edges it contains. A *cycle* is a path that begins and ends at the same vertex in which no edge is repeated, and all vertices other than the starting and ending vertex are distinct. If a graph G has a cycle, the *girth* of G (notated $g(G)$) is defined as the length of the shortest cycle of G; otherwise, $g(G) = \infty$. A graph G is *connected* if for every pair of distinct vertices $a, b \in V(G)$, there exists a path from a to b. If there is a path from a to b with $a, b \in V(G)$, then the *distance from a to b* is the length of the shortest path from a to b and is denoted $d(a, b)$. If there is not a path between a and b, $d(a, b) = \infty$. If $S = \{d(a, b) | a, b \in V(G)\}$, then the *diameter* of G is $diam(G) = \sup(S)$. If G_1 and G_2 are graphs, an *isomorphism* is a bijection $\phi : V(G_1) \to V(G_2)$ such that a—b in G_1 if and only if $\phi(a)$—$\phi(b)$ in G_2. If such a function exists, we say G_1 and G_2 are *isomorphic*. Finally, a graph G is *finite* if $V(G)$ is finite.

All images in figures were generated by [6]

Throughout, R will denote a commutative ring with identity.

3 The Cozero-Divisor Graph

[1] is currently the only published literature concerning the cozero-divisor graph of a ring. Here we will provide several fundamental results, similar to those proved for other graphical depictions of rings, which have not yet been addressed.

Theorem 2.10 in [1] states that if $Z(R) \neq W(R)$, then $\Gamma'(R)$ is finite if and only if R is finite, where $W(R) = W(R)^* \cup \{0\}$. We provide a proof for a more generalized statement.

Theorem 3.1. *$\Gamma'(R)$ is finite if and only if R is finite.*

Proof. Suppose $\Gamma'(R)$ is finite. Then $|W(R)^*| < \infty$ implies that $|Z(R)| < \infty$; hence, $|R| < \infty$ by [2, Theorem 2.2]. The other direction is trivial. □

The authors of [1] did not investigate direct products of rings, but in fact $\Gamma'(R)$ preserves connectedness over a direct product.

Theorem 3.2. *Let $R \cong R_1 \times R_2 \times \cdots \times R_n$, where R_i is a commutative ring for all $i \in \{1, 2, \dots, n\}$. Let $x, y \in R$ with $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$. If x_i—y_i in $\Gamma'(R_i)$ for some $i \in \{1, 2, \dots, n\}$, then x—y in $\Gamma'(R)$.*

Proof. Suppose x is not adjacent to y. Then without loss of generality, $x \in (y)$. There exists $z \in R$ such that $zy = x = (z_1y_1, z_2y_2, \dots, z_ny_n) = (x_1, x_2, \dots, x_n)$. Thus $x_i = z_iy_i$ for all $i \in \{1, 2, \dots, n\}$, and hence x_i is not adjacent to y_i in $\Gamma'(R_i)$ for all $i \in \{1, 2, \dots, n\}$. □

The converse does not hold. If x—y in $\Gamma'(R_1 \times R_2 \times \cdots \times R_n)$, it is possible that x_i is not adjacent to y_i for all $i \in \{1, 2, \dots, n\}$. For example, in $\Gamma'(\mathbb{Z}_{16} \times \mathbb{Z}_{16})$, $(2, 4)$—$(4, 2)$, but 2 is not adjacent to 4 in $\Gamma'(\mathbb{Z}_{16})$. In fact, $\Gamma'(\mathbb{Z}_{16})$ is empty.

Corollary 3.3. *Let R_i be a commutative ring for all $i \in \{1, 2, \dots, n\}$. If a cycle exists in $\Gamma'(R_i)$ for some $i \in \{1, 2, \dots, n\}$, then a cycle exists in $\Gamma'(R)$, where $R \cong R_1 \times R_2 \times \cdots \times R_n$.*

Proof. Suppose a_i—b_i—$\cdots$—c_i—a_i is a cycle in $\Gamma'(R_i)$. Then $(0, 0, \dots, a_i, \dots, 0)$—$(0, 0, \cdots, b_i, \dots, 0)$—$\dots$—$(0, 0, \dots, c_i, \dots, 0)$—$(0, 0, \dots, a_i, \dots, 0)$ is a cycle in $\Gamma'(R)$. □

In [1], Afkhami and Khashyarmanesh introduced $\Gamma'(R)$ primarily as a dual to the zero-divisor graph. As such, most of their results concern similarities between the two graphs, as well as basic graph-theoretic properties of $\Gamma'(R)$. Since the graph is built on fundamental relationships between principal ideals, it seems likely that the structure of $\Gamma'(R)$ should relay nontrivial algebraic information about the ring, so studying it on its own could prove fruitful. Before we begin this approach, however, we observe that $\Gamma'(R)$ is not the most efficient method of displaying principal ideal relationships in graph form, so we introduce a more concise analog.

4 The Reduced Cozero-Divisor Graph

It is clear from the definition of the cozero-divisor graph that any two points that generate the same ideal will play similar roles within the structure of the graph. This next theorem demonstrates this fact.

Theorem 4.1. *Let $x, y \in W(R)^*$. If $(x) = (y)$, then x is not adjacent to y in $\Gamma'(R)$, and for all $z \in W(R)^*$, x—z if and only if y—z.*

Proof. Suppose $(x) = (y)$. Then $(x) \subseteq (y)$, so x is not adjacent to y. If z is not adjacent to x, then $(z) \subseteq (x)$ or $(x) \subseteq (z)$. Hence, $(z) \subseteq (y)$ or $(y) \subseteq (z)$, so z is not adjacent to y. Similarly, if y is not adjacent to z, then x is not adjacent to z. □

This tells us that any two points that generate the same ideal will have exactly the same set of neighbors. In this way, $\Gamma'(R)$ is somewhat redundant in its portrayal of relationships between principal ideals. The inclusion of multiple generators of the same ideal serves only to complicate the graph as the rings get larger.

This fact motivates our definition of a more efficient analog to $\Gamma'(R)$: the *reduced cozero-divisor graph of* R, $\Gamma^*(R)$. The graph is defined as follows. Let $\Omega(R)$ designate the set of principal ideals of R, and let $\Omega(R)^* = \Omega(R) \setminus \{(0), R\}$. (In other words, $\Omega(R)^*$ is the set of nontrivial principal ideals of R.) Then $V(\Gamma^*(R)) = \Omega(R)^*$, and (a)—(b) if and only if $(a) \not\subseteq (b)$ and $(b) \not\subseteq (a)$. Since the point set of $\Gamma^*(R)$ is the principal ideals themselves and not elements of R, the redundancies of $\Gamma'(R)$ are eliminated.

There are significant advantages to studying reduced cozero-divisor graphs as opposed to the cozero-divisor graphs themselves; first and foremost, as seen in Figure 2, $\Gamma^*(R)$ is typically a much simpler graph that provides the same information regarding principal ideal relationships.

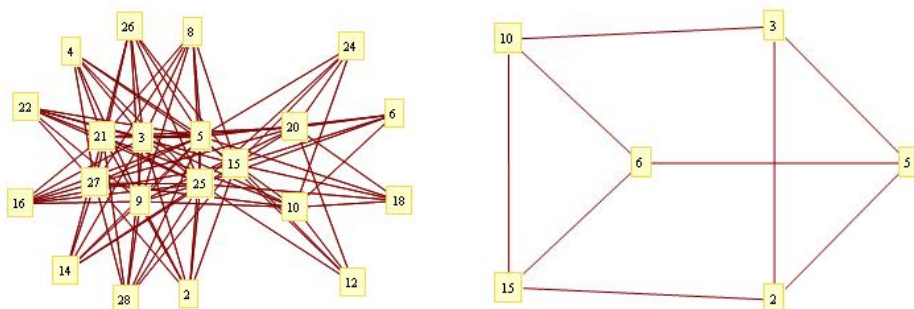

Figure 2: $\Gamma'(\mathbb{Z}_{30})$ and $\Gamma^*(\mathbb{Z}_{30})$

Additionally, examining trends in connectedness and cycles becomes much more interesting; for instance, if $a, b, c, d \in W(R)^*$ with $(a) = (b) \neq (c) = (d)$, and $(a) \not\subseteq (c)$ and $(c) \not\subseteq (a)$, then a—c—b—d—a is a (rather uninteresting) cycle in $\Gamma'(R)$, whereas the only conclusion we can draw in $\Gamma^*(R)$ is that (a)—(c). As a result, only less trivial cycles and connections will appear in $\Gamma^*(R)$.

Finally, as will be seen in Section 5, the reduced cozero-divisor graph of an finite commutative ring with identity has a unique relationship to the decomposition of that ring into local rings and fields that the cozero-divisor graph does not. This shows that $\Gamma^*(R)$ is more tied to the structure of R than $\Gamma'(R)$.

The next few results comment on the relationship between the connectedness of $\Gamma'(R)$ and $\Gamma^*(R)$.

Theorem 4.2. *(1) If* $|\,\Omega(R)^*\,| > 1$, *then* $\Gamma^*(R)$ *is connected if and only if* $\Gamma'(R)$ *is connected. (2) If* $|\,\Omega(R)^*\,| = 1$, *then* $\Gamma'(R)$ *is connected if and only if* $|W(R)^*| = 1$.

Proof. (1) ($\Rightarrow$) Suppose $\Gamma^*(R)$ is connected and let $a, b \in V(\Gamma'(R))$ with $a \neq b$. If $(a) \neq (b)$, then there is a path from (a) to (b) in $\Gamma^*(R)$ such that (a)—(c_1)—(c_2)— $\cdots$—(c_n)—(b). Thus, a—c_1—c_2— $\cdots$—c_n—b is a path in $\Gamma'(R)$. If $(a) = (b)$, then choose $c \in W(R)^*$ such that (a)—(c) in $\Gamma^*(R)$. Then $a - c - b$ in $\Gamma'(R)$, so $\Gamma'(R)$ is connected.

($\Leftarrow$) Suppose $\Gamma'(R)$ is connected. Then for all $a, b \in V(\Gamma'(R))$, $a \neq b$, there exist $c_1, c_2, \ldots, c_n$ such that a—c_1—c_2—$\cdots$—c_n—b is a path in $\Gamma'(R)$. Thus, (a)—(c_1)—(c_2)—$\cdots$—(c_n)—(b) is a path in $\Gamma^*(R)$, and $\Gamma^*(R)$ is connected.

(2) (⇒) Suppose $|W(R)^*| > 1$. Since $\Gamma'(R)$ is connected, we can choose $a, b \in W(R)^*$ with $a \neq b$ such that a—b. Then for $(a), (b) \in \Omega(R)^*$, $(a) = (b)$. However, since a—b, $a \notin (b)$ and $b \notin (a)$, a contradiction. Therefore, $\Gamma'(R)$ is not connected.

(⇐) Trivial. □

The following result follows immediately from the definitions.

Proposition 4.3. *$\Gamma^*(R)$ is empty if and only if for any $(a), (b) \in \Omega(R)^*$, $(a) \subseteq (b)$ or $(b) \subseteq (a)$.*

Theorem 4.4. *$\Gamma^*(R)$ is empty if and only if $\Gamma'(R)$ is empty.*

Proof. (⇒) If $\Gamma^*(R)$ is empty, then $(x) \subseteq (y)$ or $(y) \subseteq (x)$ for all $(x), (y) \in \Omega(R)^*$. Let $x \in \Gamma'(R)$. Then $(x) \in \Omega(R)^*$. If $|V(\Gamma^*(R))| = 1$, then $(a_i) = (a_j)$ for all $a_i, a_j \in W(R)^*$. So, $\Gamma'(R)$ is empty. If $|V(\Gamma^*(R))| > 1$, then for all $(y) \in \Omega(R)^*$, $(x) \subseteq (y)$ or $(y) \subseteq (x)$ by Proposition 4.3. Therefore, for all $y \in W(R)^*$, $y \in (x)$ or $x \in (y)$. So, $\Gamma'(R)$ is empty.

(⇐) Trivial. □

Theorem 4.5. *$diam(\Gamma^*(R)) \leq diam(\Gamma'(R))$.*

Proof. Let a_0—a_1—$\cdots$—a_k be a path of length k in $\Gamma'(R)$. If $(a_i) \neq (a_j)$ for all distinct $i, j \in \{0, 1, \ldots, k\}$, then (a_0)—(a_1)—$\cdots$—(a_k) is a path of length k in $\Gamma^*(R)$. If $(a_i) = (a_j)$ for some $i, j \in \{0, 1, \ldots, k\}$, then (a_0)—$\cdots$—(a_i)—(a_{j+1})—$\cdots$—(a_k) is a path of length k or less in $\Gamma^*(R)$. Thus, $diam(\Gamma^*(R)) \leq diam(\Gamma'(R))$. □

Note that $diam(\Gamma^*(R))$ is not necessarily equal to $diam(\Gamma'(R))$; as seen in Figure 3, $diam(\Gamma'(\mathbb{Z}_{14})) = 2$, whereas $diam(\Gamma^*(\mathbb{Z}_{14})) = 1$.

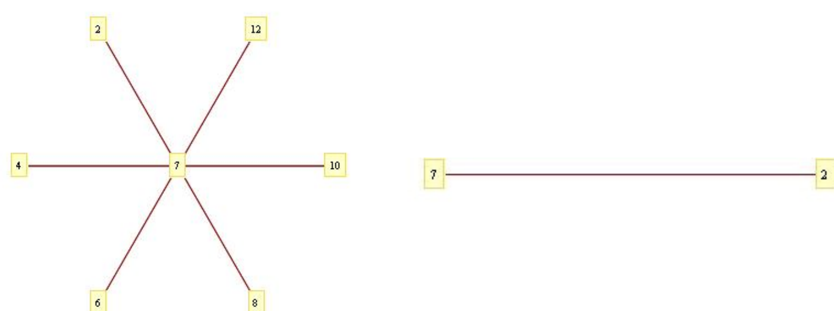

Figure 3: $\Gamma'(\mathbb{Z}_{14})$ and $\Gamma^*(\mathbb{Z}_{14})$

Observe that if $\Gamma^*(R)$ has a cycle, then $\Gamma'(R)$ will have a cycle as well (namely, the generators of the ideals in the cycle of $\Gamma^*(R)$.) However, the converse is not necessarily true. For example, $\Gamma'(\mathbb{Z}_{12})$ has a cycle while $\Gamma^*(\mathbb{Z}_{12})$ does not (see Figure 4).

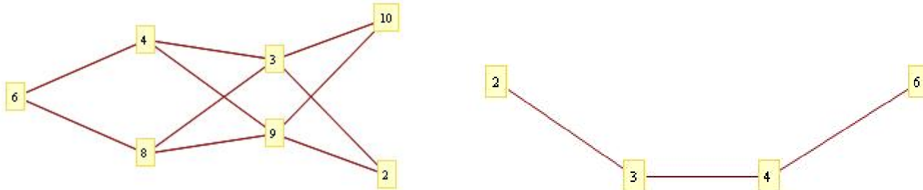

Figure 4: $\Gamma'(\mathbb{Z}_{12})$ and $\Gamma^*(\mathbb{Z}_{12})$

Theorem 4.6. *Suppose $\Gamma'(R)$ has a cycle.*
(1) If $\Gamma^*(R)$ has a cycle, then $g(\Gamma'(R)) \leq g(\Gamma^*(R))$.
(2) If $\Gamma^*(R)$ does not have a cycle, then $g(\Gamma'(R)) = 4$.

Proof. (1) If (a_1)—(a_2)—$\cdots$—(a_n)—(a_1) is the smallest cycle in $\Gamma^*(R)$, then a_1—a_2—$\cdots$—a_n—a_1 is a cycle in $\Gamma'(R)$. So, $g(\Gamma'(R)) \leq g(\Gamma^*(R))$.

(2) Suppose a_1—a_2—$\cdots$—a_n—a_1 is a cycle in $\Gamma'(R)$. Note that $a_1, a_2, \ldots, a_n$ do not all generate distinct ideals because then there would be a cycle in $\Gamma^*(R)$. Now suppose there does not exist $i \in \{1, 2, \ldots, n\}$ such that $(a_i) = (a_{i+2})$. Then for some ideal $(a_j) = (a_k)$ with $j < k$ such that $(a_i) \neq (a_l)$ for all distinct $i, l \in \{j, j+1, j+2, \ldots, k-1, k\}$ (other than $i = j$ and $l = k$), (a_j)—(a_{j+1})—$\cdots$—(a_k) is a cycle in $\Gamma^*(R)$, a contradiction. Therefore, there exists an $i \in \{1, 2, \ldots, n\}$ such that $(a_i) = (a_{i+2})$. By Theorem 4.1, a_{i+2}—a_{i-1}. Hence, a_{i-1}—a_i—a_{i+1}—a_{i+2}—a_{i-1} is a cycle of length 4 in $\Gamma'(R)$, so $g(\Gamma'(R)) \leq 4$. If there is a cycle of length 3 in $\Gamma'(R)$, say b_1—b_2—b_3—b_1, then clearly, (b_1)—(b_2)—(b_3)—(b_1) is a cycle in $\Gamma^*(R)$, a contradiction. Therefore, $g(\Gamma'(R)) = 4$. □

Theorem 4.7. *If $\Gamma'(R)$ has a cycle of odd length, then $\Gamma^*(R)$ has a cycle.*

Proof. We will prove this claim by induction as follows: The base case is the statment that if $\Gamma'(R)$ has a cycle of length 3, then $\Gamma^*(R)$ has a cycle, and the inductive hypothesis is the statement that if $\Gamma'(R)$ has a cycle of length n implies that $\Gamma^*(R)$ has a cycle, then $\Gamma'(R)$ having a cycle of length $n+2$ should imply that $\Gamma^*(R)$ has a cycle.

If a_1—a_2—a_3—a_1 in $\Gamma'(R)$, then (a_1)—(a_2)—(a_3)—(a_1) is a cycle in $\Gamma^*(R)$. Now assume that if a_1—a_2—$\cdots$—a_n—a_1 is a cycle in $\Gamma'(R)$ where n is odd, then $\Gamma^*(R)$ has a cycle. Consider a cycle a_1—a_2—$\cdots$—a_n—a_{n+1}—a_{n+2}—a_1 in $\Gamma'(R)$. If all a_i generate distinct ideals for $i \in \{1, 2, \ldots, n\}$, then (a_1)—(a_2)—$\cdots$—(a_n)—(a_{n+1})—(a_{n+2})—(a_1) is a cycle in $\Gamma^*(R)$. Suppose that at least two elements generate the same ideal. If $\Gamma^*(R)$ does not have a cycle, then by the proof of the previous theorem, there exists k such that $(a_k) = (a_{k+2})$. Since the cycle is finite, without loss of generality, suppose $(a_n) = (a_{n+2})$. Then a_1—a_2—$\cdots$—a_n—a_1 is a cycle in $\Gamma'(R)$. Thus by our inductive hypothesis, $\Gamma^*(R)$ has a cycle. □

5 $\Gamma^*(R)$ and Ring Decomposition

We begin with a generalization of Theorem 3.2 to the reduced cozero-divisor ring, which states that the adjacencies of the graph of a product of rings depend on those of the component rings.

Theorem 5.1. *Let $R \cong R_1 \times R_2 \times \cdots \times R_n$, where R_i is a commutative ring for all $i \in \{1, 2, \ldots, n\}$. Let $x, y \in R$ with $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$. If (x_i)—(y_i) in $\Gamma^{*\prime}(R_i)$ for some $i \in \{1, 2, \ldots, n\}$, then (x)—(y) in $\Gamma^*(R)$.*

Proof. Suppose (x) is not adjacent to (y). Then without loss of generality, $x \in (y)$. Then there exists $z \in R$ such that $zy = x = (z_1y_1, z_2y_2, \ldots, z_ny_n) = (x_1, x_2, \ldots, x_n)$. So $x_i = z_iy_i$ for all $i \in \{1, 2, \ldots, n\}$, and hence, (x_i) is not adjacent to (y_i) for all i. □

As in the cozero-divisor graph, the converse does not hold. In $\Gamma^*(\mathbb{Z}_{16} \times \mathbb{Z}_{16})$, $((2, 4))$—$((4, 2))$, but (2) is not adjacent to (4) in $\Gamma^*(\mathbb{Z}_{16})$.

Before we continue, it is important to note that the 0 and 1 elements may differ from ring to ring. However, for simplicity's sake we will continue to notate them as 0 to 1, and we leave it to the reader to understand from context which elements are being referred to.

All finite rings can be decomposed such that $R \cong R_1 \times R_2 \times \cdots \times R_n$ for $i \in \{1, 2, \ldots, n\}$ where each R_i is a local ring or a field [3]. The following theorems give information about ring and graph isomorphisms when R is decomposed as above.

Lemma 5.2. *Let $R = F_1 \times F_2 \times \cdots \times F_n$, where F_i is a field for all $i \in \{1, 2, \ldots, n\}$, and $S = \{(a_1, a_2, \ldots, a_n) | a_i \in \{0, 1\}\} \setminus \{0_R, 1_R\}$. Then $\Omega(R)^* = \{(s) : s \in S\}$. In particular, $|\,\Omega(R)^*\,| = 2^n - 2$.*

Proof. Let $b = (b_1, b_2, \ldots b_n)$. If $b \in S$, then $(b) \in \Omega(R)^*$. Now let $b \in R$ such that $(b) \in \Omega(R)^*$. Now, $b_i = 0$ for at least one i, else $(b) = R$. Similarly, $b_i \neq 0$ for some i as well. Now let $r \in R$ with $r = (r_1, r_2, \ldots, r_n)$ be defined by

$$r_i = \begin{cases} 1 & \text{if } b_i \neq 0 \\ 0 & \text{if } b_i = 0 \end{cases}$$

Then $r \in S$. Now, $rb = b$, so $b \in (r)$. To show $r \in (b)$, define $c \in R$ by

$$c_i = \begin{cases} b_i^{-1} & \text{if } b_i \neq 0 \\ 0 & \text{if } b_i = 0 \end{cases}$$

Hence, $cb = r$, so $r \in (b)$. Therefore, $(b) = (r)$, which implies $(b) \in \{(s) | s \in S\}$. Thus, $\Omega(R)^* = S$.

Note that if $x, y \in S$ with $x \neq y$ then $(x) \neq (y)$. Hence, there are 2^n choices for a generator consisting of a 0 or 1 in each component. Since $((0, 0, \ldots, 0))$, $((1, 1, \ldots, 1)) \notin \Omega(R)^*$, $|\,\Omega(R)^*\,| = 2^n - 2$. □

Theorem 5.3. *Let $R_1 \cong F_1 \times F_2 \times \cdots \times F_n$ and $R_2 \cong G_1 \times G_2 \times \cdots \times G_m$, where F_i and G_j are fields for all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$. Then $n = m$ if and only if $\Gamma^*(R_1) \cong \Gamma^*(R_2)$.*

Proof. ($\Rightarrow$) Assume that $n = m$. By Lemma 5.2, $V(\Gamma^*(R_1)) = \{((a_1, \ldots, a_n)) | a_i \in \{0, 1\}\} \setminus \{R_1, (0)\}$, $V(\Gamma^*(R_2)) = \{((b_1, \ldots, b_n)) | b_i \in \{0, 1\}\} \setminus \{R_2, (0)\}$, and $|V(\Gamma^*(R_1))| = |V(\Gamma^*(R_2))|$. Now define $f : V(\Gamma^*(R_1)) \to V(\Gamma^*(R_2)$ by $f(((a_1, \ldots, a_n))) = ((b_1, \ldots, b_n))$ where

$$b_i = \begin{cases} 1 & \text{if } a_i \neq 0 \\ 0 & \text{if } a_i = 0 \end{cases}$$

This is clearly a well-defined bijection. Let $S_1 = \{(a_1, a_2, \ldots, a_n) | a_i \in \{0,1\}\} \setminus \{0_{R_1}, 1_{R_1}\} \subseteq R_1$, and let $S_2 = \{(b_1, b_2, \ldots, b_n) | b_i \in \{0,1\}\} \setminus \{0_{R_2}, 1_{R_2}\} \subseteq R_2$, and let $x, y \in S_1$ with $x \neq y$. Assume (x) is adjacent to (y). Then $(x) \nsubseteq (y)$ and $(y) \nsubseteq (x)$. Thus, there are some i, j such that $x_i = 0$ but $y_i = 1$, and $y_j = 0$ but $x_j = 1$. Now $f((x)) = (c)$ and $f((y)) = (d)$, where $c_i = 0$ if $x_i = 0$ and 1 otherwise, and $d_i = 0$ if $y_i = 0$ and 1 otherwise. Hence $(c) = f((x)) \nsubseteq (d)$, and $(d) = f((y)) \nsubseteq (c)$, so $f((x))$—$f((y))$. Similarly, $f((x))$—$f((y))$ implies (x)—(y). Therefore, $\Gamma^*(R_1) \cong \Gamma^*(R_2)$.
($\Leftarrow$) Assume $\Gamma^*(R_1) \cong \Gamma^*(R_2)$. Then by Lemma 5.2, $2^n - 2 = |V(\Gamma^*(R_1))| = |V(\Gamma^*(R_2))| = 2^m - 2$. Therefore, $m = n$. □

An example of this are $\mathbb{Z}_{14}$ and $\mathbb{Z}_{15}$, both of which can be decomposed into a direct product of two fields: $\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7$ and $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$.

Figure 5: $\Gamma^*(\mathbb{Z}_{14})$ and $\Gamma^*(\mathbb{Z}_{15})$

If a ring decomposes into a direct product of fields, we can additionally determine the diameter of its reduced cozero-divisor graph based on the length of the product.

Theorem 5.4. *Let $R \cong F_1 \times F_2 \times \cdots \times F_n$, where F_i is a field for all $i \in \{1, 2, \ldots, n\}$. Then*

$$diam(\Gamma^*(R)) = \begin{cases} 1 & \text{if } n = 2 \\ 2 & \text{if } n > 2 \end{cases}$$

Proof. If $n = 2$, then $\Omega(R)^* = \{((1,0)), ((0,1))\}$, and $((1,0))$—$((0,1))$. So, $diam(\Gamma^*(R)) = 1$. If $n > 2$, then $d = ((1,1,0,\ldots,0))$ is not adjacent to $e = ((1,0,0,\ldots,0))$, so $diam(\Gamma^*(R)) > 1$. Note that if $R = F_1 \times F_2 \times \ldots \times F_n$, then $(x) \in \Omega(R)^*$ implies that x has at least one component equal to zero; additionally, if $(x) \neq (y)$, then there must exist $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, such that $x_i = 0$ and $y_j = 0$. If $x = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$, with a 1 in the jth position (or $y = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$, with a 1 in the ith position), then (x)—(y). Otherwise, let $(c) \in \Omega(R)^*$ be defined by

$$c_k = \begin{cases} 1 & \text{if } k = i \text{ or } k = j \\ 0 & \text{otherwise} \end{cases}$$

Then (x)—(c)—(y), so $diam(\Gamma^*(R)) = 2$. □

When we the consider decomposition of a ring into a direct product of local rings, the results are not as clean. However, we can determine if the graphs are isomorphic in the specific case when those local rings are of the form $\mathbb{Z}_{p^a}$, where p is prime.

Lemma 5.5. *Let* $R \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}$ *and* $S = \{(c_1, c_2, \ldots, c_n) : c_i \in \{0, 1, p_i, \ldots, p_i^{a_i-1}\}\} \setminus \{0, 1\}$. *Then* $\Omega(R)^* = \{(s) | s \in S\}$. *In particular,* $|\,\Omega(R)^*\,| = [\prod_{i=1}^{n}(a_i + 1)] - 2$.

Proof. Let $y \in S$. Clearly, $(y) \in \Omega(R)^*$. Let $x \in R$ such that $(x) \in \Omega(R)^*$. Choose $r = (r_1, r_2, \ldots, r_n)$ such that

$$r_i = \begin{cases} 0 & \text{if } x_i = 0 \\ gcd(x_i, p_i^{a_i}) & \text{if } x_i \neq 0 \end{cases}$$

Clearly, $r \in S$. We want to show that $(r) = (x)$. Since $r_i | x_i$, there exists $d_i \in \mathbb{Z}_{p_i^{a_i}}$ such that $r_i d_i = x_i$ for each nonzero x_i. We now have $rd = x$, where $d = (d_1, d_2, \ldots, d_n)$. Thus, $x \in (r)$. Since $r_i = gcd(x_i, p_i^{a_i})$, there exist $m_i, n_i \in \mathbb{Z}$ with $x_i m_i + p_i^{\alpha_i} n_i = r_i$. Modulo $p_i^{a_i}$, this equation reduces to $x_i m_i = r_i$. Hence, $r \in (x)$. Therefore, $(x) \in \{(s) | s \in S\}$, and $\Omega(R)^* = \{(s) | s \in S\}$. Note that all elements of the form $(c_1, c_2, \ldots, c_n)$ are distinct and that there are $a_i + 1$ choices for the i^{th} coordinate. Since we disregard R and (0), $|\,\Omega(R)^*\,| = [\prod_{i=1}^{n}(a_i + 1)] - 2$. □

Theorem 5.6. *Let* R_1 *and* R_2 *be rings with* $R_1 \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}$ *and* $R_2 \cong \mathbb{Z}_{q_1^{b_1}} \times \mathbb{Z}_{q_2^{b_2}} \times \cdots \times \mathbb{Z}_{q_m^{b_m}}$, *where* p_i *and* q_i *are prime integers and* $a_i, b_j > 1$ *for* $i \in \{1, 2, \ldots, n\}$ *and* $j \in \{1, 2, \ldots, m\}$. *If* $n = m$ *and* $a_1, a_2, \ldots, a_n$ *is a permutation of* $b_1, b_2, \ldots, b_n$, *then* $\Gamma^*(R_1) \cong \Gamma^*(R_2)$.

Proof. Without loss of generality, suppose $a_i = b_i$ for $i \in \{1, 2, \ldots, n\}$. By Lemma 5.5,

$$V(\Gamma^*(R_1)) = \{((c_1, \ldots, c_n)) : c_i \in \{0, 1, p_i, p_i^2, \ldots, p_i^{a_i-1}\}\} \setminus \{R_1, (0)\} = S_1$$
$$V(\Gamma^*(R_2)) = \{((c_1, \ldots, c_n)) : c_i \in \{0, 1, q_i, q_i^2, \ldots, q_i^{a_i-1}\}\} \setminus \{R_2, (0)\} = S_2$$

Let $f : V(\Gamma^*(R_1)) \to V(\Gamma^*(R_2))$ defined by $f((c_1, \ldots, c_n)) = (z)$ where $(c_1, c_2, \ldots, c_n) \in S_1$ by

$$z = \begin{cases} 0 & \text{if } c_i = 0 \\ q_i^{\alpha} & \text{if } c_i = p_i^{\alpha} \end{cases}$$

Note that by Lemma 5.5, f will be onto; furthermore, $|V(\Gamma^*(R_1))| = |V(\Gamma^*(R_2))|$, so f is one-to-one.

Let $S_1 = \{(c_1, c_2, \ldots, c_n) | c_i \in \{0, 1, p_i, \ldots, p_i^{a_i-1}\}\} \setminus \{0_{R_1}, 1_{R_1}\}$ and $S_2 = \{(c_1, c_2, \ldots, c_n) | c_i \in \{0, 1, q_i, \ldots, q_i^{a_i-1}\}\} \setminus \{0_{R_2}, 1_{R_2}\}$ and $x, y \in S_1$. Then $(x), (y) \in \Omega(R_1)^*$. If $f((x))$ is not adjacent to $f((y))$, then without loss of generality, $f((x)) \subseteq f((y))$. There exist $m, n \in S_2$ such that $f((x)) = (m)$ and $f((y)) = (n)$. Since $(m) \subseteq (n)$, there does not exist i such that either $n_i = 0$ and $m_i \neq 0$, or $n_i = q_i^{\alpha}$ and $m_i = q_i^{\beta}$ with $\alpha > \beta$. Consider $f^{-1}(f((x))) = (x)$ and $f^{-1}(f((y))) = (y)$. By definition of f, there does not exist i such that $y_i = 0$ and $x_i \neq 0$ or $y_i = p_i^{\alpha}$ and $x_i = p_i^{\beta}$ with $\alpha > \beta$. Therefore, $(x) \subseteq (y)$, and (x) is not adjacent to (y). Thus, (x)—(y) implies $f((x))$—$f((y))$. Similarly, if $f((x))$—$f((y))$, then (x)—(y). □

Consider $\mathbb{Z}_{72} \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2}$ and $\mathbb{Z}_{200} \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_{5^2}$, and observe that $\Gamma^*(\mathbb{Z}_{72}) \cong \Gamma^*(\mathbb{Z}_{200})$ (Figure 7).

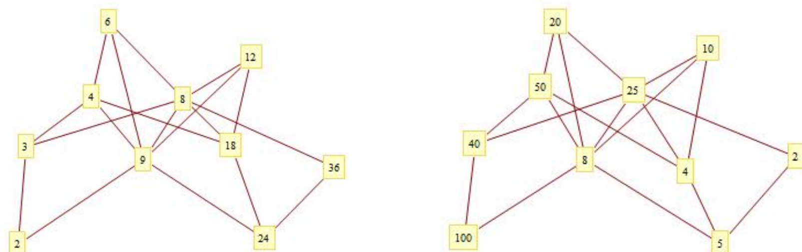

Figure 7: $\Gamma^*(\mathbb{Z}_{72})$ and $\Gamma^*(\mathbb{Z}_{200})$

There are many possibilities for future research into this topic. This could include proving the converse of Theorem 5.6, and investigating more general decompositions as well. Also, more research could be done on the characterization of graph-theoretic properties that are realizable as reduced cozero-divisor graphs, such as the cases in which $\Gamma^*(R)$ has a cycle. Additionally, connections may be able to be made between $\Gamma^*(R)$ and $\Gamma(R)$, along the lines of research in [1].

References

[1] Afkhami, M. and Khashyarmanesh, K., The cozero-divisor graph of a commutative ring, *S.E. Asian Bull. Math*, to appear.

[2] Anderson, D. F. and Livingston, P., The zero-divisor graph of a commutative ring, *J. of Algebra*, **217** (1999), 434-447.

[3] Dummit, David S., and Foote, Richard M., *Abstract Algebra, 3rd Ed.* (2004), John Wiley and Sons, Inc.

[4] Harris, John M. et. al. *Combinatorics and Graph Theory* (2000), Springer-Verlag New York Inc.

[5] Hungerford, Thomas W. *Algebra* (1996), Springer-Verlag New York Inc.

[6] MATHEMATICA, Wolfram Software.

[7] Zariski, Oscar and Samuel, Pierre. *Commutative Algebra, Volume I* (1958), D. Van Nostrand Company, Inc.