On the unitary Cayley graph of a finite ring

Reza Akhtar
Department of Mathematics
Miami University
reza@calico.mth.muohio.edu

Megan Boggess
Columbia Union College
meganboggess@gmail.com

Tiffany Jackson-Henderson
St. Augustine's College
tjackhend@yahoo.com

Isidora Jiménez
Mills College
ijimenez@mills.edu

Rachel Karpman
Scripps College
rkarpman@scrippscollege.edu

Amanda Kinzel
Department of Mathematics
Purdue University
asphilli@math.purdue.edu

Dan Pritikin
Department of Mathematics
Miami University
pritikd@muohio.edu

Submitted: May 16, 2009; Accepted: Sep 7, 2009; Published: Sep 18, 2009
Mathematics Subject Classification: 05C25, 05C30

Abstract

We study the unitary Cayley graph associated to an arbitrary finite ring, determining precisely its diameter, girth, eigenvalues, vertex and edge connectivity, and vertex and edge chromatic number. We also compute its automorphism group, settling a question of Klotz and Sander. In addition, we classify all planar graphs and perfect graphs within this class.

1 Introduction

Given an integer n, consider the graph $Cay(\mathbb{Z}_n, \mathbb{Z}_n^*)$ with vertex set $\mathbb{Z}_n$ (the integers modulo n), with vertices x and y adjacent exactly when $x - y$ is a unit in (the ring) $\mathbb{Z}_n$. These so-called *unitary Cayley graphs* have been studied as objects of independent interest (see, for example, [2], [3], [7], [8], [9]) but are of particular relevance in the study of graph representations, begun in [5] and continued in many other papers. A graph is said to be *representable modulo* n if it is isomorphic to an induced subgraph of $Cay(\mathbb{Z}_n, \mathbb{Z}_n^*)$; the central problem in graph representations is to determine the smallest positive n modulo which a given graph G is representable. It is natural, then, to study unitary Cayley graphs in the hope of gaining insight into the graph representation problem.

A generalization of unitary Cayley graphs presents itself readily: given a finite ring R (commutative, with unit element $1 \neq 0$), one may define $G_R = Cay(R, R^*)$ to be the ring whose vertex set is R, with an edge between x and y if $x - y \in R^*$. This construction was introduced in [7] and [8], although it does not appear to have been considered in [9].

This article began as a project to address the question of computing the automorphism group $Aut(Cay(\mathbb{Z}_n, \mathbb{Z}_n^*))$, first raised by Klotz and Sander in [9]. We soon realized that it was more natural to consider this question in the context of (unitary Cayley graphs of) finite rings. In this article we give a complete answer to this question; moreover, we extend the results of [9] to the setting of finite rings and explore various other graph-theoretic properties not considered there. Our proofs emphasize the dependence of results on the underlying algebraic structure of the rings concerned; in some cases, these provide a considerable simplification of the Klotz-Sander proofs. We hope that the use of some algebra will provide a more cohesive approach to further study of these graphs.

A key observation is the following: since R is a finite ring, it is Artinian, and hence $R \cong R_1 \times \ldots \times R_t$, where each R_i is a finite local ring with maximal ideal $\mathfrak{m}_i$. Since $(u_1, \ldots, u_t)$ is a unit of R if and only if each u_i is a unit in R_i^*, we see immediately that G_R is the conjunction (sometimes called tensor product or Kronecker product) of the graphs $G_{R_1}, \ldots, G_{R_t}$. Moreover, if $x, y \in R_i$, $\{x, y\}$ is an edge of G_{R_i} if and only if $x - y \notin \mathfrak{m}_i$. It follows immediately that each G_{R_i} is a complete balanced multipartite graph whose partite sets are the cosets of $\mathfrak{m}_i$ in (the additive group) R_i. This perspective allows us, for example, to give a simple, explicit computation of the eigenvalues of the graphs G_R (see Section 10). In future work we hope to generalize the study of graph representations to this broader setting.

Part of this research was carried out in the SUMSRI program, held at Miami University during the summer of 2008. We thank Miami University, the National Security Agency, and the National Science Foundation for their support of the first six authors. We also thank the referee for suggestions which helped improve this paper.

2 Algebraic Background and Basic Properties

Throughout this paper, all rings mentioned are commutative with unit element $1 \neq 0$. Let R be a finite ring. Since R is Artinian, the structure theorem [4, p. 752, Theorem 3] implies that $R \cong R_1 \times \ldots \times R_t$, where each R_i is a finite local ring with maximal ideal $\mathfrak{m}_i$; this decomposition is unique up to permutation of factors. We denote by k_i the (finite) residue field $R_i/\mathfrak{m}_i$, $\pi_i : R_i \to k_i$ the quotient map, and $f_i = |k_i|$. We also assume (after appropriate permutation of factors) that $f_1 \leqslant f_2 \leqslant \ldots \leqslant f_t$. This notation will be maintained throughout the paper whenever R is mentioned as a finite (or more generally Artinian) ring.

The following proposition is well-known, but we include it here for the sake of completeness.

Proposition 2.1. *Let S be a finite local ring with maximal ideal $\mathfrak{m}$. Then there exists a prime p such that $|R|$, $|\mathfrak{m}|$ and $|R/\mathfrak{m}|$ are all powers of p.*

Proof.
Since $k = R/\mathfrak{m}$ is a field, its order must be equal to p^e for some prime p and integer $e \geqslant 1$. Since R is finite, Nakayama's Lemma implies that as long as $\mathfrak{m}^i \neq 0$, $\mathfrak{m}\mathfrak{m}^i = \mathfrak{m}^{i+1} \neq \mathfrak{m}^i$; that is, $\mathfrak{m}^{i+1}$ is a strict subset of $\mathfrak{m}^i$. Since R is finite, this implies that in the chain $R \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \ldots$, there is some i such that $\mathfrak{m}^i = 0$. Then for all $j \geqslant 1$, $|\mathfrak{m}^{j-1}/\mathfrak{m}^j|$ is a k-vector space, so its order is a power of p. Then descending induction on j shows that $|\mathfrak{m}^j|$ is a power of p for all $j \geqslant 0$. □

We note in particular that the nilradical of a local ring R (the ideal $\mathfrak{N}_R$ of nilpotent elements) is simply the (unique) maximal ideal of R.

It is well-known that if R is an Artinian ring, then $R \cong R_1 \times \ldots \times R_t$, where each R_i is an Artinian local ring. Furthermore, $R^* = R_1^* \times \ldots \times R_t^*$, and hence two vertices $x = (x_1, \ldots, x_t)$, $y = (y_1, \ldots, y_t)$ are adjacent if and only if $x_i - y_i \in R_i^*$ for all $i = 1, \ldots, t$. Equivalently, x is adjacent to y if and only if for each $i = 1, \ldots, t$, $x_i - y_i \notin \mathfrak{m}_i$; that is, $\pi_i(x_i) \neq \pi_i(y_i)$.

The following are some basic consequences of this definition:

Proposition 2.2.

- *Let R be any ring. Then G_R is a regular graph of degree $|R^*|$.*
- *Let S be a local ring with maximal ideal $\mathfrak{m}$. Then G_S is a complete multipartite graph whose partite sets are the cosets of $\mathfrak{m}$ in S. In particular, G_S is a complete graph if and only if S is a field.*
- *If R is any Artinian ring and $R \cong R_1 \times \ldots \times R_t$ as a product of local rings, then $G_R = \bigwedge_{i=1}^t G_{R_i}$. Hence, G_R is a conjunction of complete multipartite graphs.*

Proof.
The first statement follows from the fact that the neighborhood of any vertex a is $\{a + u : u \in R^*\}$. For the second statement, simply note that $x, y \in S$ are adjacent if and only if $x - y \notin \mathfrak{m}$ and that S is a field if and only if $\mathfrak{m} = 0$. The third statement follows from the fact that $R^* \cong R_1^* \times \ldots \times R_t^*$. □

Remark.

For any $r \in R$, the map $z \mapsto z + r$ defines an automorphism G_R; similarly, if $u \in R^*$, $z \mapsto uz$ is also an automorphism of G_R. We will compute the full group $Aut(G_R)$ in Section 4.

Throughout this paper, we use $N(v)$ for the neighborhood of a vertex (that is, the set of vertices adjacent to v) and $N(u, v)$ for the number of common neighbors of the vertices u and v. We now give a formula for the latter in G_R:

Proposition 2.3. *Suppose* $a = (a_1, \ldots, a_t)$ *and* $b = (b_1, \ldots, b_t)$ *are vertices of* G_R. *Let* $I = \{i : 1 \leqslant i \leqslant t,\ \pi_i(a_i) = \pi_i(b_i)\}$ *and* $J = \{1, \ldots, t\} - I$. *Then*

$$N(a, b) = |R| \prod_{i\in I}(1 - \frac{1}{f_i}) \prod_{j\in J}(1 - \frac{2}{f_j})$$

Proof.

If $c = (c_1, \ldots, c_t)$ is adjacent to both a and b, then for each $k = 1, \ldots, t$, c_i may be any element such that $\pi_i(c_i) \notin \{\pi_i(a_i), \pi_i(b_i)\}$. If $\pi_i(a_i) = \pi_i(b_i)$, there are $\dfrac{f_i - 1}{f_i}|R_i|$ choices for c_i, and if $\pi_i(a_i) \neq \pi_i(b_i)$, there are $\dfrac{f_i - 2}{f_i}|R_i|$ choices for c_i. In total, then, there are $\prod_{i\in I}(1 - \frac{1}{f_i})|R_i| \cdot \prod_{j\in J}(1 - \frac{2}{f_j})|R_j| = |R| \prod_{i\in I}(1 - \frac{1}{f_i}) \prod_{j\in J}(1 - \frac{2}{f_j})$ choices for c. □

Corollary 2.4. *Let* R *be an Artinian ring and* $x, y \in G_R$. *Then* $N(x) = N(y)$ *if and only if* $x - y \in \mathfrak{N}_R$.

Some questions about properties of unitary Cayley graphs are best viewed as purely combinatorial questions about conjunctions of complete balanced multipartite graphs. We will adopt this persective at various points later in this article. Sometimes we can simplify things even further, as explained in the next paragraph.

Consider two vertices v, w of a graph G to be equivalent when $N(v) = N(w)$. Then, following [6] we define the *reduction* of G to be the graph G_{red} whose vertex set is the set of equivalence classes of vertices (as defined above), and whose edges consist of pairs $\{A, B\}$ of equivalence classes with the property that $A \cup B$ induces a complete bipartite subgraph of G.

Proposition 2.5. *Let* R *be an Artinian ring. Then the reduction* $(G_R)_{red} \cong G_{R_{red}}$ *where* $R_{red} = R/\mathfrak{N}_R$ *is the (ring-theoretic) reduction of* R.

Proof.

First, write $R = R_1 \times \ldots \times R_t$ as a product of local rings. Then $\mathfrak{N}_R = \mathfrak{N}_{R_1} \times \ldots \times \mathfrak{N}_{R_t} = \mathfrak{m}_1 \times \ldots \times \mathfrak{m}_t$ and so $R_{red} = R_1/\mathfrak{m}_1 \times \ldots \times R_t/\mathfrak{m}_t$ is a product of fields. Moreover, it is clear from the description of adjacency above that two vertices $(a_1, \ldots, a_t)$, $(b_1, \ldots, b_t)$ of G_R have the same neighborhood if and only if $a_i - b_i \in \mathfrak{m}_i$ for all $i = 1, \ldots, t$. This implies that vertices of $(G_R)_{red}$ correspond to elements of $R_{red} = R_1/\mathfrak{m}_1 \times \ldots \times R_t/\mathfrak{m}_t$. Since adjacency is defined by the same rule in both graphs, it follows that $(G_R)_{red} \cong G_{R_{red}}$. □

Proposition 2.5 allows us to convert general questions about unitary Cayley graphs of finite rings to corresponding questions about finite reduced rings (i.e. products of fields).

3 Diameter and Girth

In the following we use diam(G) and gr(G) (respectively) to denote the diameter and girth of a graph G.

Theorem 3.1. *Let $R = R_1 \times \ldots \times R_t$ be an Artinian ring. Then*

$$\text{diam } G_R = \begin{cases} 1 & \text{if } t = 1 \text{ and } R \text{ is a field} \\ 2 & \text{if } t = 1 \text{ and } R \text{ is not a field} \\ 2 & \text{if } t \geqslant 2, f_1 \geqslant 3 \\ 3 & \text{if } t \geqslant 2, f_1 = 2, f_2 \geqslant 3 \\ \infty & \text{if } t \geqslant 2, f_1 = f_2 = 2. \end{cases}$$

Proof.

If $t = 1$, then by Proposition 2.2, G_R is complete if R is a field, and is a complete multipartite graph (with at least two partite sets) if R is not a field. In the first case, G_R has diameter 1; in the second case, it has diameter 2. Now suppose $t \geqslant 2$ and $f_1 > 2$. Then $f_i \geqslant 3$ for all $i = 1, \ldots, t$, so given distinct vertices $a = (a_1, \ldots, a_t)$, $b = (b_1, \ldots, b_t)$, select elements $c_i \in R_i$, $i = 1, \ldots, t$, such that $\pi_i(c_i) \notin \{\pi_i(a_i), \pi_i(b_i)\}$. Then $c = (c_1, \ldots, c_t)$ is a common neighbor of a and b and so diam $G_R \leqslant 2$. Obviously G_R is not complete in this case, so diam $G_R = 2$.

If $t \geqslant 2$ and $f_1 = 2$, observe that the vertices $(0, 0, \ldots, 0)$ and $(1, 0, \ldots, 0)$ are neither adjacent nor do they share a common neighbor; hence diam $G_R \geqslant 3$. If, moreover, $f_2 = 2$, then there is a no path in G_R between these same two vertices, so G_R is disconnected. On the other hand, if $f_2 \geqslant 3$, consider distinct vertices $a = (a_1, \ldots, a_t)$ and $b = (b_1, \ldots, b_t)$ such that $d(a, b) \geqslant 3$. In particular, $\pi_1(a_1) \neq \pi_1(b_1)$ and for some $i \geqslant 2$, $\pi_i(a_i) = \pi_i(b_i)$. Now define $c = (c_1, \ldots, c_t)$, $d = (d_1, \ldots, d_t)$ as follows: for each i, $1 \leqslant i \leqslant t$, if $\pi_i(a_i) = \pi_i(b_i)$, pick $c_i, d_i \in R_i$ such that $\pi_i(c_i)$, $\pi_i(d_i)$, and $\pi_i(a_i) = \pi_i(b_i)$ are distinct; if $\pi_i(a_i) \neq \pi_i(b_i)$, set $d_i = b_i$ and $c_i = a_i$. Then a, d, c, b is a path of length 3, so diam $G_R = 3$. □

Theorem 3.2. $$\text{gr } G_R = \begin{cases} 3 & \text{if } f_1 \geqslant 3 \\ 6 & \text{if } R \cong \mathbb{Z}_2^r \times \mathbb{Z}_3 \text{ for some } r \geqslant 1 \\ \infty & \text{if } R \cong \mathbb{Z}_2^r \text{ for some } r \geqslant 1 \\ 4 & \text{otherwise.} \end{cases}$$

Proof.

Suppose first that $f_1 \geqslant 3$. Then any three vertices $a = (a_1, \ldots, a_t)$, $b = (b_1, \ldots, b_t)$, $c = (c_1, \ldots, c_t)$ such that $\pi_i(a_i)$, $\pi_i(b_i)$, and $\pi_i(c_i)$ are distinct for all $i = 1, \ldots, t$ induce a triangle, and so gr $G_R = 3$.

We next consider the case $t = 1$, $f_1 = 2$. If $R \cong \mathbb{Z}_2$, clearly gr $G_R = \infty$. Otherwise, R is not a field, so G_R is a complete bipartite graph with partite sets of size $|\mathfrak{m}_1| \geqslant 2$, and hence gr $G_R = 4$.

Now suppose $f_1 = 2$ and $t \geqslant 2$. Then G_R is a bipartite graph, so gr $(G_R) \geqslant 4$. Let $a = (0, \ldots, 0)$ and $b = (1, \ldots, 1)$. If R_i is not a field for some $i \geqslant 1$, then $|\mathfrak{m}_i| \geqslant 2$, so choosing $0 \neq x \in \mathfrak{m}_i$, define $c = (c_1, \ldots, c_t)$ and $d = (d_1, \ldots, d_t)$ by setting, for each $j = 1, \ldots, t$, $c_j = \delta_{ij}x$ and $d_j = 1 + \delta_{ij}x$. Then a, b, c, d, a is a 4-cycle, and so gr $(G_R) = 4$. If R_j is a field for all $j \geqslant 1$ and $|R_i| \geqslant 4$ for some i, choose elements $c_i, d_i \in R_i$ such that $\pi_i(c_i), \pi_i(d_i)$ are distinct elements of $k - \{0, 1\}$. For $j \neq i$, define $c_j = a_j$ and $d_j = b_j$, and let $c = (c_1, \ldots, c_t)$, $d = (d_1, \ldots, d_t)$. Then a, b, c, d, a is a 4-cycle, and so gr $(G_R) = 4$ in this case, too.

We are now reduced to the case that $R \cong \mathbb{Z}_2^r \times \mathbb{Z}_3^s$ for some r, s, $r + s \geqslant 2$. Since G_R is bipartite, it contains no odd cycles. To simplify notation in the following discussion we use the notation x_m to represent an m-tuple each of whose coordinates is x (in the appropriate ring). If $s \geqslant 2$, then $(0_r, 0_s), (1_r, 1_s), (0_r, 2, \ldots, 2, 0), (1_r, 1, \ldots, 1, 2), (0_r, 0_s)$ defines a 4-cycle in G_R. If $s = 1$, the vertex sequence $(0_r, 0), (1_r, 1), (0_r, 2), (1_r, 0)$ $(0_r, 1), (1_r, 2), (0_r, 0)$ defines a 6-cycle, so gr $G_R \leqslant 6$. If a, b, c, d, a were a cycle of length 4 in G_R, then $a_i = c_i$ for all i and $b_i = d_i$ $(1 \leqslant i \leqslant r)$, so in particular $a_{r+1} \neq c_{r+1}$, $b_{r+1} \neq d_{r+1}$, and so $S = \{a_{r+1}, c_{r+1}\}$ and $T = \{b_{d+1}, d_{r+1}\}$ are (by virtue of the adjacency conditions) *disjoint* subsets of R_{r+1}, each of cardinality 2. However, $|R_{r+1}| = 3$, so this is a contradiction. Thus, gr $G_R = 6$. The last case to consider is $R \cong \mathbb{Z}_2^r$, but in this case, $G_R \cong 2^{r-1} K_2$ and hence gr $G_R = \infty$. □

Corollary 3.3. *The number of triangles in* G_R *is* $\frac{|R|^3}{6} \prod_{i=1}^{t} (1 - \frac{1}{f_i})(1 - \frac{2}{f_i})$.

Proof.
If $f_1 = 2$, then by Proposition 3.2, G_R is triangle-free, so the claim holds in this case. If $f_1 \geqslant 3$, then given a vertex $a \in R$, by Proposition 2.2 there are $|R^*| = |R| \prod_{i=1}^{t} (1 - \frac{1}{f_i})$ choices for an adjacent vertex b. Now, Proposition 2.3 implies that there are $|R| \prod_{i=1}^{t} (1 - \frac{2}{f_i})$ choices for a third vertex which is a common neighbor of both a and b. Since any such triangle may be formed in 6 distinct ways, the total number of triangles is $\frac{|R|^3}{6} \prod_{i=1}^{t} (1 - \frac{1}{f_i})(1 - \frac{2}{f_i})$. □

4 Automorphisms

In this section we compute the group $Aut(G_R)$ when R is a finite ring. We begin by reducing the problem to the case of reduced rings.

Lemma 4.1. *Let R be a finite ring and $n = |\mathfrak{N}_R|$.*
Then there is an isomorphism $f : Aut(G_R) \xrightarrow{\cong} Aut(G_{R_{red}}) \times (S_n)^{|R/\mathfrak{N}_R|}$.

Proof.

It follows from Corollary 2.4 that any $\sigma \in Aut(G_R)$ permutes the cosets of $\mathfrak{N}_R$ in R; in particular, σ induces an automorphism $\bar{\sigma} \in Aut(G_{R_{red}})$. Moreover, if one fixes an enumeration $x_1, \ldots, x_n$ of the elements of $\mathfrak{N}_R$ and a set of coset representatives $\mathcal{R} = \{a_C\}_{C \in R/\mathfrak{N}_R}$, then for each such coset $C = a_C + \mathfrak{N}_R$ of $\mathfrak{N}_R$ in R, $\sigma(C) = b_C + \mathfrak{N}_R$ for some representative $b_C \in \mathcal{R}$; in particular, there is a permutation $\sigma_C \in S_n$ such that for each $i = 1, \ldots, n$, $\sigma(a_C + x_i) = b_C + x_{\sigma_C(i)}$. We now define $f(\sigma) = (\bar{\sigma}, \prod_{C \in R/\mathfrak{N}_R} \sigma_C)$; it is immediate that f is a homomorphism and that Ker $f = 1$, so f is injective.

Now suppose we are given $\psi = (\tau, \prod_{C \in R/\mathfrak{N}_R} \phi_C) \in Aut(G_{R_{red}}) \times \prod_{C \in R/\mathfrak{N}_R} S_n$. By construction, each element of R may be written uniquely as $a_C + x_j$ for some $C \in R/\mathfrak{N}_R$ and $1 \leqslant j \leqslant n$. Define b_C to be the (unique) element of $\mathcal{R}$ satisfying $\tau(a_C + \mathfrak{N}_R) = b_C + \mathfrak{N}_R$. Now define $\sigma \in Aut(G_R)$ by $\sigma(a_C + x_j) = b_C + \phi_C(x_j)$. Then $f(\sigma) = \psi$ and so f is surjective. ☐

For rings $S_1, \ldots, S_m$, we define the *number of leading zeros* of an element $s = (s_1, \ldots, s_m) \in S_1 \times \ldots \times S_m$ to be $\max\{\ell \geqslant 0 : s_1 = \ldots = s_\ell = 0\}$.

We now turn to the case of reduced rings.

Theorem 4.2. *Let $s \geqslant 1$, and suppose $r_1, \ldots, r_s$ are prime powers such that $2 \leqslant r_1 < \ldots < r_s$. For each $i = 1, \ldots, s$, let $n_i \geqslant 1$ be an integer, and consider the ring $R = \prod_{i=1}^{s} (F_i)^{n_i}$, where F_i denotes the field with r_i elements. Then $Aut(G_R) \cong \prod_{i=1}^{s} S_{r_i} \times \prod_{i=1}^{s} S_{n_i}$.*

Proof.

The idea behind the proof is to identify certain "obvious" automorphisms of G_R and then prove that any automorphism σ coincides with one of these, using the property that for any two vertices $u, v \in G_R$, $N(\sigma(u), \sigma(v)) = N(u, v)$.

Since R is reduced, any (set) map $f : R \to R$ which fixes all but one of the local factors and permutes the elements of the remaining factor induces an automorphism of G_R. Similarly, a map $f : R \to R$ which is the identity on $(F_i)^{n_i}$ for $i \neq i_0$ and permutes the n_{i_0} factors of the form F_{i_0} induces an automorphism of G_R. Let $H \subseteq Aut(G_R)$ be the subgroup generated by maps of either of these two types. It remains to check that in fact $H = Aut(G_R)$. Observe that translations, i.e. automorphisms of the form $z \mapsto z + a$ for some fixed $a \in R$, are compositions of maps of the first type.

To this end, suppose $\sigma \in Aut(G_R)$. Composing with a translation, we may assume without loss of generality that $\sigma(0) = 0$. Our goal is prove that, after composition with maps in H, $\sigma(a) = a$ for all $a \in R$. We do this by downward induction on the number ℓ of leading zeros in the coordinate representation for a, the base case being $\ell = m$; that is, $a = 0$.

Suppose by induction that $\sigma(a) = a$ for all a with more than ℓ leading zeros, and suppose $b = (b_{1,1}, \ldots, b_{1,n_1}, \ldots, b_{s,1}, \ldots, b_{s,n_s}) \in R$ has ℓ leading zeros. Suppose the leftmost nonzero coordinate in b is the (i,j) coordinate. Define b' to have the same coordinates as b except for the (i,j) coordinate, which is 0. Observe that if $c \in R$ has at most ℓ leading zeros, then $|N(b,b')| \leqslant |N(c,b')|$ by Proposition 2.3, with equality if and only if c and b differ only in the (i,k) coordinate for some k, $1 \leqslant k \leqslant j$. By induction, $\sigma(b') = b'$ and $\sigma(b)$ has at most ℓ leading zeros. Moreover, since σ is an automorphism, $N(b,b') = N(\sigma(b),b')$, so by the inequality above, $\sigma(b)$ differs from b only in the (i,k) coordinate, where $1 \leqslant k \leqslant j$. By applying an automorphism in H of the second type, we may assume that $k = j$, and after applying an automorphism of the first type, $\sigma(b) = b$. This completes the induction. □

5 Connectivity

Proposition 5.1. *Let R be any finite ring, and let $\kappa(G_R)$ and $\kappa'(G_R)$ denote (respectively) the vertex-connectivity and edge-connectivity of its unitary Cayley graph. Then $\kappa(G_R) = \kappa'(G_R) = |R^*|$.*

Proof.
We argue following the reasoning in [9], Theorem 4. According to a theorem of Watkins [10], the vertex connectivity of a regular edge-transitive graph is equal to its degree of regularity. We show that G_R is edge-transitive by observing that for any edge $\{u,v\}$ the automorphism $x \mapsto (v-u)^{-1}(x-u)$ maps u to 0 and v to 1. Hence $\kappa(G_R) = |R^*|$. Since $\kappa(G_R) \leqslant \kappa'(G_R) \leqslant |R^*|$ by [11, Theorem 4.1.9], it follows that $\kappa(G_R) = \kappa'(G_R) = |R^*|$. □

6 Clique Number, Chromatic Number, and Independence Number

For a graph G, we denote by $\bar{G}$ its complement, $\omega(G)$ its clique number, $\alpha(G)$ its independence number, and $\chi(G)$ its chromatic number.

Proposition 6.1. *Let R be a finite ring. Then $\omega(G_R) = \chi(G_R) = f_1$ and $\omega(\overline{G_R}) = \chi(\overline{G_R}) = \alpha(G_R) = \dfrac{|R|}{f_1}$.*

Proof.
Choose elements $r_{ij} \in R_i$, $i = 1,\dots,t$, $j = 1,\dots,f_1$ such that for each $i = 1,\dots,t$ and $j \neq j'$, $\pi_i(r_{ij}) \neq \pi_i(r_{ij'})$. Then, setting $a_j = (r_{1j},\dots,r_{tj})$ for each $j = 1,\dots,f_1$, it is easily seen that $C = \{a_1,\dots,a_{f_1}\}$ is a clique and $\omega(G_R) \geqslant f_1$. Now consider the ideal $I = \mathfrak{m}_1 \times R_2 \ldots \times R_t \subseteq R$. There are precisely f_1 cosets of I in R, each of which corresponds to an independent subset of G_R. By assigning each coset a distinct color and coloring all vertices within that coset the same color, we have constructed a proper coloring of G_R. Hence, $\chi(G_R) \leqslant f_1$. Since $f_1 \leqslant \omega(G_R) \leqslant \chi(G_R) \leqslant f_1$, we have $\omega(G_R) = \chi(G_R) = f_1$.

Since the ideal I constructed above corresponds to an independent set in G_R, we have $\alpha(G_R) = \omega(\overline{G_R}) \geqslant |I| = |R|/f_1$. We now construct a coloring of $\overline{G_R}$ by elements of I as follows: given $b = (b_1, \ldots, b_n) \in R$, fix a clique C in G_R as above and let c_b be the unique element of C such that $b - c_b \in I$; define a vertex coloring $f : R \to I$ by $f(b) = b - c_b$. Then $f(b) = f(d)$ implies that $b - d = c_d - c_b$. If $c_d = c_b$, then $b = d$; so assume $c_d \neq c_b$. Then by construction, $c_d - c_b \in R^*$, so $b - d \in R^*$, and hence b is not adjacent to d in $\overline{G_R}$. Thus f is a proper coloring, showing that $\chi(\overline{G_R}) \leqslant |I| = |R|/f_1$, as desired. □

Corollary 6.2. *Let R be a finite ring. Then G_R is f_1-partite.*

7 Edge Chromatic Number

We next derive a result concerning the edge chromatic number $\chi'(G_R)$.

Theorem 7.1. *Let R be a finite ring. Then*

$$\chi'(G_R) = \begin{cases} |R^*| + 1 & \text{if } |R| \text{ is odd} \\ |R^*| & \text{if } |R| \text{ is even.} \end{cases}$$

Proof.
Since G_R is $|R^*|$-regular, $\chi'(G_R) \geqslant |R^*|$, and by Vizing's Theorem, $\chi'(G_R) \leqslant |R^*| + 1$. Suppose $|R|$ is odd, so G_R has no 1-factor. Then in any proper edge-coloring of G_R, each color class must miss some vertex x. Hence there are $|R^*|$ colors used on edges incident at x, plus the color of that class used elsewhere; hence, $\chi'(G_R) = |R^*| + 1$.

Now suppose $|R|$ is even. By Proposition 2.1, at least one of the local rings in the decomposition $R \cong R_1 \times \ldots \times R_t$ has even cardinality. In particular, this means that for any unit $u = (u_1, \ldots, u_t) \in R^*$, $|u| = \text{lcm}(|u_1|, \ldots, |u_t|)$ is even, where by $|u|$ (or $|u_i|$) we mean the order of u as an element of the additive abelian group R (respectively, R_i).

Let $V = \{v \in R^* : |v| = 2\}$ and $E_V = \{\{r, r + v\} : v \in V\} \subseteq E(G_R)$. We observe that there are exactly $|V|$ edges of E_V incident at every vertex of G_R. Now construct a proper coloring of $E(G)$ as follows: fix a bijection $h : V \to \{1, \ldots, |V|\}$ and, for each $v \in V$ and $r \in R$, color the edge $\{r, r + v\}$ with color $h(v)$. Now let $U' = R^* - V$; note that for each $u \in U'$, $u \neq -u$. Choose $U = \{u_1, \ldots, u_m\} \subseteq U'$ such that for all $u \in U'$, exactly one of u, $-u$ is in U; thus, $|U| = \dfrac{|R^*| - |V|}{2}$. Now for each u_j, $j = 1, \ldots, m$, let $a_1 + < u_j >, \ldots, a_s + < u_j >$ be the (distinct) cosets of $< u_j >$ in R. For each $k = 0, \ldots, |u_j| - 1$, color the edge $\{a_i + ku_j, a_i + (k + 1)u_j\}$ with color $|V| + 2j - 1$ if k is odd or color $|V| + 2j$ if k is even. It is easy to check that this procedure defines a proper edge-coloring of G with $2|U| + |V| = |R^*|$ colors. □

8 Planarity

The following is immediate from definitions:

Lemma 8.1. *Let G be a bipartite graph. Then $G \wedge K_2 \cong 2G$. In particular, G is planar if and only if $G \wedge K_2$ is planar.*

Our result on planarity is:

Theorem 8.2. *Let R be a finite ring. Then G_R is planar if and only if R is one of the following rings: $(\mathbb{Z}/2\mathbb{Z})^s$, $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^s$, $\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^s$, or $\mathbb{F}_4 \times (\mathbb{Z}/2\mathbb{Z})^s$. (Here $\mathbb{F}_4$ is the field with four elements and $s \geqslant 0$ may assume any integer value.)*

Proof.
Clearly, $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are the only rings with fewer than 4 elements, so henceforth let R be a finite ring such that G_R is planar and $|R| \geqslant 4$.

If $f_1 = 2$, then $R \cong R_1 \times \ldots \times R_t$ is bipartite by Corollary 6.2 and as such is triangle-free. By a well-known result (see for example [11, Theorem 6.1.23]), planarity of R forces $|E(R)| \leqslant 2|R| - 4$; that is, $|R^*| \leqslant 4 - \dfrac{8}{|R|}$ or $|R^*| \leqslant 3$. Now if S is a local ring, $|S^*| \geqslant \dfrac{|S|}{2}$; hence, $|S^*| = 1$ if and only if $S \cong \mathbb{Z}/2\mathbb{Z}$. Moreover, $R^* = R_1^* \times \ldots \times R_t^*$, so the condition $|R^*| \leqslant 3$ forces $R \cong S \times (\mathbb{Z}_2)^s$ for some $s \geqslant 0$ and some local ring S with $|S^*| \leqslant 3$. Since $|S| \leqslant 6$ and $|S|$ must be a prime power, the only possibilities are $S = \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}$ (with any $s \geqslant 0$), or $S = \mathbb{F}_4$ (with any $s \geqslant 1$). It is easy to check by hand that for each of these choices of S, both G_S and $G_{S \times \mathbb{Z}/2\mathbb{Z}}$ are planar. Since the graph $G_{S \times \mathbb{Z}/2\mathbb{Z}}$ is guaranteed to be bipartite by Corollary 6.2, planarity of $S \times (\mathbb{Z}_2)^s$ follows from Lemma 8.1 by induction.

Now suppose $f_1 \geqslant 3$. Then (cf. [11, Theorem 6.1.23]) planarity of $R \cong R_1 \times \ldots \times R_t$ forces $|E(R)| \leqslant 3|R| - 6$, which implies $|R^*| \leqslant 5$. However, this time each of the local factors R_i satisfies $|R_i^*| \geqslant \dfrac{2}{3}|R_i|$; in particular, if $|R_i^*| = 2$, then $|R_i| = 3$ and hence $R_i \cong \mathbb{Z}/3\mathbb{Z}$, which is impossible since $f_1 \geqslant 3$. If $|R^*| = 3$, then $R \cong \mathbb{F}_4$, and if $|R^*| = 4$, then $R \cong \mathbb{Z}/5\mathbb{Z}$. Clearly $G_{\mathbb{F}_4} \cong K_4$ is planar but $G_{\mathbb{Z}/5\mathbb{Z}} \cong K_5$ is not. □

9 Perfectness

Let R be an Artinian ring. In this section, we classify which of the graphs G_R are perfect. As before, fix a decomposition $R \cong R_1 \times \ldots \times R_t$ as a product of local rings. We note that our proof, while following the outline of the analogous result in Section 3 of [9], differs somewhat in that it avoids use of the Fuchs-Sinz result [8] on longest induced cycles.

If $t = 1$ then by Proposition 2.2 G_R is complete multipartite and hence is perfect. If $f_1 = 2$ then by Corollary 6.2 G_R is bipartite and hence perfect. We assume henceforth that $f_1 \geqslant 3$. Our main tool is the Strong Perfect Graph Theorem.

Theorem 9.1. *[3] A graph G is perfect if and only if neither G nor $\bar{G}$ contains an induced odd cycle.*

Lemma 9.2. *Suppose $t \geqslant 3$. Then G_R is not perfect.*

Proof.

For each $i = 1, \ldots, t$, fix elements $a_i^{(0)}, a_i^{(1)}, a_i^{(2)}$ such that the values of $\pi_i(a_i^{(j)})$, $j = 0, 1, 2$, are mutually distinct. For convenience, we assume $a_i^0 = 0$, $a_i^{(1)} = 1$ for all i and write $c_i = a_i^{(2)}$. Then given a triple $t = (a_1^{(x_1)}, a_2^{(x_2)}, a_3^{(x_3)}) \in R_1 \times R_2 \times R_3$, where $0 \leqslant x_j \leqslant 2$ for $j = 1, 2, 3$, define its *extension* $ext(t) = (w_1, \ldots, w_t) \in R$ by $w_i = a_i^{(x_j)}$, where $0 \leqslant j \leqslant 2$ is the unique integer such that $i \equiv j (\bmod 3)$. Then the vertices $ext(0,0,0), ext(1,1,1), ext(0, c_2, c_3), ext(1,1,0), ext(c_1, c_2, 1)$ induce a 5-cycle in G_R. □

Hence we are reduced to the case that $R \cong R_1 \times R_2$ where R_1, R_2 are local.

Lemma 9.3. *If R is of the above form, then $\overline{G_R}$ does not contain any induced odd cycle of length $\geqslant 5$.*

Proof.

For contradiction, suppose that $\overline{G_R}$ has an induced cycle of length $2m+1$ for some $m \geqslant 2$, and that the order of consecutive vertices around the cycle is $a_1, \ldots, a_{2m+1}, a_1$. For each i, let $a_i = (a_{i,1}, a_{i,2})$. Then, since a_i is adjacent to a_{i+1} (taken modulo 2m+1) in $\overline{G_R}$, at least one of $\pi_1(a_{i,1}) = \pi_1(a_{i+1,1})$ or $\pi_2(a_{i,2}) = \pi_2(a_{i+1,2})$ must hold. For convenience, call the edge $\{a_i, a_{i+1}\}$ *red* if the first statement holds or *blue* otherwise. Because a_{i-1} is also adjacent to a_i but not to a_{i+1}, $\{a_{i-1}, a_i\}$ cannot be the same color as $\{a_i, a_{i+1}\}$. Hence, consecutive edges around the cycle alternate between red and blue; however, this leads to a contradiction because the cycle has odd length. □

Lemma 9.4. *If R is of the above form, then G_R does not contain any induced odd cycle of length $\geqslant 5$.*

Proof.

Suppose first that $m \geqslant 3$ and the subgraph induced by some vertices $a_i = (a_{i,1}, a_{i,2})$, $i = 1, \ldots, 2m+1$ is a cycle. As above, assume that the order of consecutive vertices around the cycle is given by $a_1, a_2, \ldots, a_{2m+1}, a_1$. After applying an appropriate automorphism of G_R, we may assume $a_1 = (0,0)$ and $a_2 = (1,1)$. Since a_3 is not adjacent to a_1, at least one of $\pi_1(a_{3,1})$, $\pi_2(a_{3,2})$ is 0. However, since a_5 is adjacent to neither a_1 nor a_3, we may assume without loss of generality that $\pi_1(a_{3,1}) = \pi_1(a_{5,1}) = 0$. On the other hand, a_5 is not adjacent to a_2, so $\pi_2(a_{5,2}) = 1$. Moreover, a_4 is adjacent to a_5, but not to a_1 or a_2, so $\pi_1(a_{4,1}) = 1$ and $\pi_2(a_{4,2}) = 0$. Also, since a_3 is adjacent to a_4, $\pi_2(a_{3,2}) \neq 0$. Finally, a_6 is not adjacent to a_1; if $\pi_1(a_{6,1}) = 0$, this contradicts its being adjacent to a_5. Hence $\pi_1(a_{6,3}) \neq 0$ and $\pi_2(a_{6,2}) = 0$, but since a_6 is not adjacent to a_2, it must be the case that $\pi_1(a_{6,2}) = 1$; this contradicts a_6 not being adjacent to a_3.

The assertion for cycles of length 5 follows from Lemma 9.3 and the fact that the complement of a 5-cycle is another 5-cycle. □

The results above now prove:

Theorem 9.5. *Let R be an Artinian ring. Then G_R is perfect if and only if $f_1 = 2$, R is local, or R is a product of two local rings.*

10 Eigenvalues

In this section, we show how to compute the eigenvalues of G_R using elementary methods. The derivation we give is much shorter and simpler than the proof in [9] (which involves Ramanujan sums) and hinges on the property that G_R is a conjunction of complete multipartite graphs.

Let R be a finite ring with local factors $R_1, \ldots, R_t$. As is standard, if A is an $n \times n$ matrix with eigenvalues $\lambda_1, \ldots, \lambda_n$ of respective multiplicities $m_1, \ldots, m_n$, we use the notation Spec $A = \begin{pmatrix} \lambda_1 & \ldots & \lambda_n \\ m_1 & \ldots & m_n \end{pmatrix}$ to describe the spectrum of A.

Lemma 10.1. *Let G and H be graphs. Suppose that $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of G and $\mu_1, \ldots, \mu_n$ are the eigenvalues of H (repetition is possible). Then the eigenvalues of $G \wedge H$ are $\lambda_i \mu_j$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$.*

Proof.
The result follows immediately from the well-known facts that $A(G \wedge H)$ is the tensor product of the matrices $A(G)$ and $A(H)$, and that the eigenvalues of a tensor product of matrices may be found by taking products of the eigenvalues of the factors. □

The fundamental results are contained in the following routine calculation:

Proposition 10.2.

- *Let F be a field with n elements. Then Spec $(G_F) = \begin{pmatrix} n-1 & -1 \\ 1 & n-1 \end{pmatrix}$.*
- *Let S be a finite local ring which is not a field, having (nonzero) maximal ideal $\mathfrak{m}$ of size m. Let $f = |S|/m$. Then Spec $(G_S) = \begin{pmatrix} -m & 0 \\ f & f(m-1) \end{pmatrix}$.*

Proof.
If F is a field with n elements, $G_F \cong K_n$. Its adjacency matrix is $A(G_F) = J_n - I_n$, where J_n is the matrix of all 1s and I_n is the identity matrix. Hence, the eigenvalues of $A(G_F)$ are each 1 less than those of J_n. To determine the latter, J_n is clearly seen to have rank 1, so 0 is an eigenvalue of multiplicity $n-1$. Moreover, the vector $[1, \ldots, 1]^T$ is clearly seen to be an eigenvector of J_n with associated eigenvalue n, which must necessarily be of multiplicity 1.

If S is a local ring with maximal ideal $\mathfrak{m} \neq 0$, then G_S is a balanced complete multipartite graph with $f = |S/\mathfrak{m}|$ partite sets, each of size $m = |\mathfrak{m}|$. In view of the regularity of G_S, it is well-known (cf. [11, Theorem 8.6.25]) that if $\lambda_1, \ldots, \lambda_n$ are eigenvalues for $A(G_S)$, then $-1-\lambda_1, \ldots, -1-\lambda_n$ are eigenvalues for $A(\overline{G_S})$. However, $\overline{G_S}$ is a disjoint union of f cliques, each of size m; hence Spec $(\overline{G_S}) = \begin{pmatrix} m-1 & -1 \\ f & f(m-1) \end{pmatrix}$ and so Spec $(G_S) = \begin{pmatrix} -m & 0 \\ f & f(m-1) \end{pmatrix}$. □

It is easily seen that these calculations, together with Lemma 10.1, may be used to compute the eigenvalues of G_R for any ring R. Since the eigenvalues of G_F are all nonzero when F is a field, the formula for the spectrum of G_R becomes quite complicated when many of the local factors of R are fields. However, if none of the local factors of R are fields, the formula takes on a rather appealing form:

Corollary 10.3. *Let R be a finite ring and suppose R has t local factors, none of which are fields. Then Spec* $(G_R) = \begin{pmatrix} (-1)^t|\mathfrak{N}_R| & 0 \\ |R_{red}| & |R| - |R_{red}| \end{pmatrix}$.

Proof.

Suppose the local factors of R are R_i, $i = 1, \ldots, t$, each R_i having maximal ideal of size $m_i > 1$ and residue field of size f_i. Then the previous calculation and Lemma 10.1 together imply

$$\text{Spec } (G_R) = \begin{pmatrix} (-1)^t \prod_{i=1}^t m_i & 0 \\ \prod_{i=1}^t f_i & |R| - \prod_{i=1}^t f_i \end{pmatrix} = \begin{pmatrix} (-1)^t|\mathfrak{N}_R| & 0 \\ |R_{red}| & |R| - |R_{red}| \end{pmatrix}.$$

□

References

[1] M. Bernstein. Representations of graphs and rings. *SUMSRI Journal*, 2008.

[2] P. Berrizbeitia and R. E. Giudici. On cycles in the sequence of unitary Cayley graphs. *Discrete Math.* **282** (2004), 1-3.

[3] M. Chudnovsky, N. Robertson, P. Seymour, and R. Thomas. *The Strong Perfect Graph Theorem. Ann. Math.* **164** (2002), 51-229.

[3] I. Dejter and R. E. Giudici. On unitary Cayley graphs. *J. Combin. Math. Combin. Comput.* **18** (1995), 121-124.

[4] D. S. Dummit and R. M. Foote. *Abstract Algebra.* Third Edition, Wiley and Sons.

[5] P. Erdős and A. B. Evans. Representations of graphs and orthogonal Latin square graphs. *J. Graph Theory* **13** (1989), no. 5, 593-595.

[6] A. B. Evans, G. Fricke, C. Maneri, T. McKee, M. Perkel. Representations of Graphs Modulo n. *Journal of Graph Theory* **18**, no. 8 (1994), 801-815.

[7] E. Fuchs. Longest induced cycles in circulant graphs. *Electronic Journal of Combinatorics* **14** (2005), no. 1, Research Paper 52.

[8] E. Fuchs and J. Sinz. Longest induced cycles in Cayley graphs. ArXiv: math/0410308v2 (2004).

[9] W. Klotz and T. Sander. Some Properties of Unitary Cayley Graphs. *Electronic Journal of Combinatorics* **14** (2007), no. 1, Research Paper 45.

[10] M. E. Watkins. Connectivity of transitive graphs. *J. Combin. Theory* **8** (1970), 23-29.

[11] D. B. West. *Graph Theory*, Second Edition. Prentice-Hall, 2000.