Canad. Math. Bull. Vol. 63 (1), 2020 pp. 58–65
http://dx.doi.org/10.4153/S0008439519000365
© Canadian Mathematical Society 2019

Spectra of Boolean Graphs Over Finite Fields of Characteristic Two

D. Scott Dillery and John D. LaGrange

Abstract. With entries of the adjacency matrix of a simple graph being regarded as elements of $\mathbb{F}_2$, it is proved that a finite commutative ring R with $1 \neq 0$ is a Boolean ring if and only if either $R \in \{\mathbb{F}_2, \mathbb{F}_2 \times \mathbb{F}_2\}$ or the eigenvalues (in the algebraic closure of $\mathbb{F}_2$) corresponding to the zero-divisor graph of R are precisely the elements of $\mathbb{F}_4 \setminus \{0\}$. This is achieved by observing a way in which algebraic behavior in a Boolean ring is encoded within Pascal's triangle so that computations can be carried out by appealing to classical results from number theory.

1 Introduction

Let R be a finite commutative ring with $1 \neq 0$. As defined in [1], the *zero-divisor graph* $\Gamma(R)$ of R is the simple graph whose vertices are given by $V(\Gamma(R)) = Z(R) \setminus \{0\}$ (the nonzero zero-divisors of R) such that distinct vertices x and y are adjacent if and only if $xy = 0$. The *adjacency matrix* of a simple graph Γ with vertices $v_1, \ldots, v_n$ is the $n \times n$ $\{0,1\}$-matrix $A(\Gamma)$ such that $A(\Gamma)(i,j) = 1$ for $1 \leq i, j \leq n$ if and only if v_i and v_j are adjacent in Γ, and an *eigenvalue* of Γ is any eigenvalue of $A(\Gamma)$ (which is necessarily real since $A(\Gamma)$ is symmetric). Note that any two adjacency matrices of Γ are similar (*e.g.*, [7, Lemma 8.1.1]), so there will be no harm in using this notation and terminology without regard for the sequence $v_1, \ldots, v_n$.

Let $\mathbb{Z}_n$, $\mathbb{F}_{p^n}$, and $R[X]$ denote the ring of integers modulo n, the finite field of order p^n, and the polynomial ring with coefficients in a ring R, respectively. Recall that a ring $R \neq \{0\}$ is *Boolean* if $x^2 = x$ for every $x \in R$, and it is well known that a finite ring R is Boolean if and only if $R \cong \mathbb{F}_2^n$ (the direct product of n factors of $\mathbb{F}_2$) for some positive integer n ([2, Theorem 8.7]). It was proved in [9, Theorem 3.4] that a commutative ring R with $1 \neq 0$ is a Boolean ring if and only if either $R \cong \mathbb{F}_2$, or $R \notin \{\mathbb{Z}_9, \mathbb{F}_3[X]/(X^2)\}$ and $\Gamma(R)$ satisfies certain *reciprocal eigenvalue properties* (namely, if λ is a real eigenvalue of $\Gamma(R)$ of multiplicity m, then either $1/\lambda$ or $-1/\lambda$ is an eigenvalue of $\Gamma(R)$ of multiplicity m; such properties are examined in the context of more general graphs in [3,12]). This result fails when computations take place within the algebraic closure of a finite field. For example, every complete zero-divisor graph of even order (*e.g.*, $\Gamma(\mathbb{Z}_{p^2})$ for any odd prime p) satisfies these reciprocal eigenvalue properties over the algebraic closure $\overline{\mathbb{F}_2}$ of $\mathbb{F}_2$ (indeed, it is easy to check that the minimal polynomial of the adjacency matrix of such a graph is $(X+1)^2$, so its only eigenvalue is $1 = -1$). Thus, a stronger result would be given by classifying Boolean

Received by the editors October 9, 2017; revised June 27, 2019.
Published online on Cambridge Core November 4, 2019.
AMS subject classification: **05C25**, 05C50, 13M99.
Keywords: zero-divisor graph, Boolean ring, eigenvalue, Pascal matrix.

https://doi.org/10.4153/S0008439519000365 Published online by Cambridge University Press

rings with respect to eigenvalues over $\overline{\mathbb{F}_2}$, and this is the objective that is accomplished in this note. Furthermore, it is shown that the adjacency matrix of the zero-divisor graph of a finite Boolean ring can be obtained by reducing the entries of a certain Pascal-type matrix modulo 2 and, while the real eigenvalues associated with finite Boolean rings remain unknown,[1] the eigenvalues over $\overline{\mathbb{F}_2}$ of zero-divisor graphs of finite Boolean rings are determined.

Throughout, the unique (up to isomorphism) Boolean ring of cardinality 2^n will often be denoted by $\mathbb{B}_{2^n}$. Also, let $\mathbb{N}$, $\mathbb{Z}$, and S_n be the positive integers, the integers, and the symmetric group on n elements, respectively. If $f \in \mathbb{Z}[X]$, then $\overline{f} \in \mathbb{F}_2[X]$ will denote the polynomial obtained by reducing the coefficients of f modulo 2.

Given any square matrix M with real entries, the characteristic polynomial of M will be denoted by C_M. If every entry of M is an integer, then let $\overline{M}$ be the $\{0,1\}$-matrix given by reducing the entries of M modulo 2. It will be stated explicitly when the entries of $\overline{M}$ are to be regarded as elements of $\mathbb{F}_2$. In this case, note that the characteristic polynomial of $\overline{M}$ in $\mathbb{F}_2[X]$ is given by $\overline{C_M}$.

2 Preliminary Results and Definitions

Let $2 \le k \in \mathbb{N}$, and consider the $(k-1)\times(k-1)$ *Pascal matrices* P_k and Q_k defined by $P_k(i,j) = \binom{i}{k-j}$ and $Q_k(i,j) = \binom{i-1}{k-j-1}$ (where $\binom{m}{n} = 0$ if $m < n$). Hence, P_k and Q_k are determined by the first k rows of Pascal's triangle. For example,

$$P_4 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 3 & 3 \end{bmatrix} \quad \text{and} \quad Q_4 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix}.$$

The sequence $L_1, L_2, \dots,$ of *Lucas numbers* is defined by the recursion $L_{n+2} = L_{n+1} + L_n$, where the initial values are given by $L_1 = 1$ and $L_2 = 3$. Let φ denote the *golden ratio* $1/2 + \sqrt{5}/2$, and set $\xi = -\varphi^{-1}$. The Binet Formula for Lucas numbers is given by $L_n = \varphi^n + \xi^n$ for every $n \in \mathbb{N}$. This formula is easily checked by noting that $\varphi + \xi = 1$, $\varphi^2 + \xi^2 = 3$, and $\varphi^{n+2} + \xi^{n+2} = (\varphi^{n+1} + \xi^{n+1})(\varphi + \xi) + (\varphi^n + \xi^n) = (\varphi^{n+1} + \xi^{n+1}) + (\varphi^n + \xi^n)$ for every $n \in \mathbb{N}$.

Given $2 \le k \in \mathbb{N}$, it is well known that the eigenvalues of Q_k are given by φ^{k-2}, $\varphi^{k-3}\xi, \dots, \varphi\xi^{k-3}, \xi^{k-2}$ (in particular, $C_{Q_k} = \prod_{j=0}^{k-2}(X - \varphi^{k-2-j}\xi^j)$ [4, (1.5)]). The following two results verify that if $k \ge 4$, then the eigenvalues of $\overline{Q_k}$ over $\overline{\mathbb{F}_2}$ (neglecting multiplicities) are precisely the elements of $\mathbb{F}_4 \setminus \{0\}$.

Lemma 2.1 *If* $2 \le k \in \mathbb{N}$, *then* $C_{Q_{k+2}} = (X^2 - L_k X + (-1)^k)C_{-Q_k}$.

Proof The equality $\varphi\xi = -1$ implies

$$(\varphi^{k-1}\xi, \varphi^{k-2}\xi^2, \dots, \varphi^2\xi^{k-2}, \varphi\xi^{k-1}) = (-\varphi^{k-2}, -\varphi^{k-3}\xi, \dots, -\varphi\xi^{k-3}, -\xi^{k-2}),$$

[1]However, the real eigenvalues of *unrestricted* zero-divisor graphs of finite Boolean rings are determined in [8, Remark 6.5].

https://doi.org/10.4153/S0008439519000365 Published online by Cambridge University Press

so

$$\begin{aligned} C_{Q_{k+2}} &= \prod_{j=0}^{k}(X-\varphi^{k-j}\xi^{j}) \\ &= (X-\varphi^{k})(X-\xi^{k})\prod_{j=1}^{k-1}(X-\varphi^{k-j}\xi^{j}) \\ &= (X-\varphi^{k})(X-\xi^{k})\prod_{j=1}^{k-1}(X+\varphi^{k-1-j}\xi^{j-1}) \\ &= \left(X^2-L_kX+(-1)^k\right)\prod_{j=0}^{k-2}(X+\varphi^{k-2-j}\xi^{j}) \\ &= \left(X^2-L_kX+(-1)^k\right)C_{-Q_k}. \end{aligned}$$ ■

Recall that the field $\mathbb{F}_4$ on four elements is the set containing 0 and the roots (in $\overline{\mathbb{F}_2}$) of $X+1$ and X^2+X+1. The next result reveals the eigenvalues of $\overline{Q_k}$ over $\overline{\mathbb{F}_2}$ for every $2 \le k \in \mathbb{N}$.

Proposition 2.2 *Let $2 \le k \in \mathbb{N}$. The eigenvalue of $\overline{Q_2}$ over $\overline{\mathbb{F}_2}$ is* 1*; the eigenvalues of $\overline{Q_3}$ over $\overline{\mathbb{F}_2}$ are the elements of $\mathbb{F}_4 \smallsetminus \{0,1\}$, and if $k \ge 4$, then the eigenvalues of $\overline{Q_k}$ over $\overline{\mathbb{F}_2}$ are the elements of $\mathbb{F}_4 \smallsetminus \{0\}$ (neglecting multiplicities).*

Proof The eigenvalues of $\overline{Q_2}$ and $\overline{Q_3}$ are easily verified. Also, Lemma 2.1 implies that if $k \ge 2$, then

$$\overline{C_{Q_{k+2}}} = \overline{(X^2-L_kX+(-1)^k)C_{-Q_k}} = (X^2+\ell X+1)\overline{C_{Q_k}}$$

for some $\ell \in \mathbb{F}_2$, so the result follows by induction, since L_2 is odd, L_3 is even, and $X^2+\ell X+1 \in \{(X+1)^2, X^2+X+1\}$ for every $\ell \in \mathbb{F}_2$. ■

Moving to zero-divisor graphs of finite Boolean rings, the following proposition expresses $C_{A(\Gamma(\mathbb{B}_{2^n}))}$ in terms of the characteristic polynomials of Pascal matrices.

Proposition 2.3 *If $2 \le n \in \mathbb{N}$, then*

$$\begin{aligned} C_{A(\Gamma(\mathbb{B}_{2^n}))} &= C_{P_n}\cdot\prod_{j=1}^{\lfloor n/2\rfloor}\left(\prod_{i=j}^{n-j}(X-\varphi^{n-i}\xi^{i})\right)^{\binom{n}{j}-\binom{n}{j-1}} \\ &= C_{P_n}\cdot\prod_{j=1}^{\lfloor n/2\rfloor} C_{(-1)^jQ_{n-2j+2}}^{\binom{n}{j}-\binom{n}{j-1}}. \end{aligned}$$

Proof By [10, Theorem 4.3], $C_{A(\Gamma(\mathbb{B}_{2^n}))} = C_{P_n}\cdot\prod_{i=1}^{n-1}(X-\varphi^{n-i}\xi^{i})^{\binom{n}{i}-1}$. Hence, the first equality follows by collecting the $\binom{n}{1}-1$ factors of the form $\prod_{i=1}^{n-1}(X-\varphi^{n-i}\xi^{i})$, and then collecting the remaining $(\binom{n}{2}-1)-(\binom{n}{1}-1) = \binom{n}{2}-\binom{n}{1}$ factors of the form $\prod_{i=2}^{n-2}(X-\varphi^{n-i}\xi^{i})$, etc. The second equality holds, since

https://doi.org/10.4153/S0008439519000365 Published online by Cambridge University Press

$$\prod_{i=j}^{n-j}(X-\varphi^{n-i}\xi^{i}) = \prod_{i=0}^{n-2j}(X-\varphi^{n-j-i}\xi^{j+i})$$
$$= \prod_{i=0}^{n-2j}(X-(-1)^{j}\varphi^{n-2j-i}\xi^{i})$$
$$= \prod_{i=0}^{m-2}(X-(-1)^{j}\varphi^{m-2-i}\xi^{i}) = C_{(-1)^{j}Q_m},$$

where $m = n - 2j + 2$. ■

By Proposition 2.3, the spectrum of $\Gamma(\mathbb{B}_{2^n})$ will be revealed once the eigenvalues of P_n are determined. As this seems to be a difficult task when working over the field of complex numbers, one may turn to the problem of finding the eigenvalues of $\overline{P_n}$ over $\overline{\mathbb{F}_2}$. In the next section, it is proved that if $3 \le n \in \mathbb{N}$ and $k = 2^n - 1$, then the eigenvalues of $\overline{P_k}$ over $\overline{\mathbb{F}_2}$ (neglecting multiplicities) are precisely the elements of $\mathbb{F}_4 \setminus \{0\}$ (Theorem 3.4). But it is also shown that the adjacency matrix of $\Gamma(\mathbb{B}_{2^n})$ is given by $\overline{P_k}$ (Theorem 3.1), and these results are used in conjunction with Proposition 2.3 to prove that a finite commutative ring R with with $1 \ne 0$ is a Boolean ring if and only if either $R \in \{\mathbb{F}_2, \mathbb{F}_2 \times \mathbb{F}_2\}$ or the eigenvalues of $\Gamma(R)$ over $\overline{\mathbb{F}_2}$ (neglecting multiplicities) are precisely the elements of $\mathbb{F}_4 \setminus \{0\}$ (Corollary 3.5).

3 Eigenvalues of $A(\Gamma(\mathbb{B}_{2^n}))$

To ease notation, if $n \in \mathbb{N}$, then set $[n] = \{1,\dots,n\}$ and $[n]^* = [n] \cup \{0\}$. Recall Lucas's Theorem, which states that if p is prime and $i, j \in \mathbb{N} \cup \{0\}$ with $i = \sum_{r=0}^{n} i_r p^r$ and $j = \sum_{r=0}^{n} j_r p^r$ ($i_r, j_r \in \{0,\dots,p-1\}$), then $\binom{i}{j} \equiv \prod_{r=0}^{n}\binom{i_r}{j_r} \pmod p$ (a short proof is given in [6, Theorem 1]). In particular, $\binom{i}{j} \equiv 1 \pmod 2$ if and only if $i_r = 1$ whenever $j_r = 1$.

Let $\operatorname{supp}(i) = \{r \in \mathbb{N}\cup\{0\} \mid i_r \ne 0\}$ be the 2*-adic support* of $i = \sum_{r=0}^{n} i_r 2^r \in \mathbb{N}\cup\{0\}$ ($i_r \in \{0,1\}$). By Lucas's Theorem, if $k \ge j$, then $\binom{i}{k-j} \equiv 1 \pmod 2$ if and only if $\operatorname{supp}(k-j) \subseteq \operatorname{supp}(i)$. (The reader may prefer to adopt binary representations of integers; *e.g.*, if $n = 3$, then the integers $i = 6$ and $k - j = 2$ can be represented by 0110 and 0100, respectively, so that the congruence $\binom{i}{k-j} \equiv 1 \pmod 2$ is evident by Lucas's Theorem.) Furthermore, if $i, j \le 2^n - 1 = k$ (so that $\operatorname{supp}(i), \operatorname{supp}(j) \subseteq [n-1]^* = \operatorname{supp}(k)$ and $\operatorname{supp}(k-h) = [n-1]^* \setminus \operatorname{supp}(h)$ for each $h \in \{i, j\}$), then the inclusion $\operatorname{supp}(k-j) \subseteq \operatorname{supp}(i)$ is equivalent to $\operatorname{supp}(k-i) \cap \operatorname{supp}(k-j) = \varnothing$. Hence, in this case, $\binom{i}{k-j} \equiv 1 \pmod 2$ if and only if $\binom{j}{k-i} \equiv 1 \pmod 2$, and it follows that $\overline{P_k}$ is symmetric. In fact, the following result holds.

Theorem 3.1 *If $2 \le n \in \mathbb{N}$ and $k = 2^n - 1$, then $\overline{P_k}$ is the adjacency matrix of $\Gamma(\mathbb{B}_{2^n})$.*

Proof The present argument requires the adjacency matrix of $\Gamma(\mathbb{B}_{2^n})$ to be well defined, so it is necessary to introduce an order on $V(\Gamma(\mathbb{B}_{2^n}))$. For this, let $\mathbb{B}_{2^n} = \prod_{r=1}^{n}\mathbb{F}_2$ be endowed with the dual-colexicographic order given by $x \le y$ if and only if either $x = y$ or $x(\max\{r \mid x(r) \ne y(r)\}) = 1$. Then the mapping $\mathbb{B}_{2^n} \to [k]^*$ given by $x \mapsto \sum_{r=1}^{n} x(r)2^{r-1}$ is an order-reversing isomorphism of linearly ordered sets;

https://doi.org/10.4153/S0008439519000365 Published online by Cambridge University Press

i.e., if $\mathbb{B}_{2^n} = \{x_0, \dots, x_k\}$ with $x_0 < \cdots < x_k$, then it is given by $x_i \mapsto k-i$ (in particular, $\sum_{r=1}^{n} x_i(r)2^{r-1} = k-i$). In this case, note that $V(\Gamma(\mathbb{B}_{2^n})) = \{x_1, \dots, x_{k-1}\}$.

Let A be the adjacency matrix of $\Gamma(\mathbb{B}_{2^n})$ that is induced by the sequence $x_1, \dots, x_{k-1}$. If $i, j \in [k-1]$, then $A(i,j) = 1$ if and only if $x_i x_j = \mathbf{0}$, if and only if $x_i(r) = 0$ whenever $x_j(r) = 1$. This holds if and only if

$$\operatorname{supp}\Big(\sum_{r=1}^{n} x_i(r)2^{r-1}\Big) \cap \operatorname{supp}\Big(\sum_{r=1}^{n} x_j(r)2^{r-1}\Big) = \varnothing,$$

i.e., $\operatorname{supp}(k-i) \cap \operatorname{supp}(k-j) = \varnothing$, if and only if $\binom{i}{k-j} \equiv 1 \pmod 2$. Therefore, $A(i,j) = 1$ if and only if $\overline{P_k}(i,j) = 1$. ■

Given a square $\{0,1\}$-matrix M, let $E(M)$ denote the multiset of eigenvalues (counting multiplicities) of M over $\overline{\mathbb{F}_2}$. The next corollary follows immediately by Proposition 2.3 and Theorem 3.1.

Corollary 3.2 *If $2 \le n \in \mathbb{N}$ and $k = 2^n - 1$, then $E(\overline{P_k}) = E(\overline{P_n}) \sqcup \big(\bigsqcup_{j=1}^{\lfloor n/2 \rfloor} \bigsqcup_{i=1}^{\binom{n}{j}-\binom{n}{j-1}} E(\overline{Q_{n-2j+2}})\big)$.*

The following lemma is the key result for determining the eigenvalues of $\Gamma(\mathbb{B}_{2^n})$, as it will be applied in the next theorem to yield the minimal polynomials of the matrices $\overline{P_{2^n-1}}$. Henceforth, the $n \times n$ identity matrix and matrix whose entries are all 1s are denoted by I_n and J_n, respectively.

Lemma 3.3 *If $2 \le n \in \mathbb{N}$ and $k = 2^n - 1$, then $\overline{P_k^3} = J_{k-1} - I_{k-1}$.*

Proof Given any $m \times m$ matrix M, recall that

$$M^s(i,j) = \sum_{t_1,\dots,t_{s-1}} M(i,t_1)M(t_1,t_2)\cdots M(t_{s-1},j)$$

for every $2 \le s \in \mathbb{N}$, where $t_1, \dots, t_{s-1}$ range through $[m]$ (it is a straightforward induction argument). Thus, for fixed $i, j \in [k-1]$, set $\rho_{t_1,t_2} = \binom{i}{k-t_1}\binom{t_1}{k-t_2}\binom{t_2}{k-j}$ so that $P_k^3(i,j) = \sum_{t_1,t_2} \rho_{t_1,t_2}$. By Lucas's Theorem, $\rho_{t_1,t_2} \equiv 1 \pmod 2$ if and only if the following three conditions are satisfied:

(i) $[n-1]^* \setminus \operatorname{supp}(t_1) \subseteq \operatorname{supp}(i)$;
(ii) $[n-1]^* \setminus \operatorname{supp}(t_2) \subseteq \operatorname{supp}(t_1)$;
(iii) $[n-1]^* \setminus \operatorname{supp}(j) \subseteq \operatorname{supp}(t_2)$.

For every $\varnothing \ne S \subseteq \operatorname{supp}(i)$ there exists a unique $t_1 \in [k-1]$ such that $[n-1]^* \setminus \operatorname{supp}(t_1) = S$, so there are $2^{|\operatorname{supp}(i)|} - 1$ integers $t_1 \in [k-1]$ that satisfy (i). For every such t_1, (ii) and (iii) hold for $t_2 \in [k-1]$ if and only if $[n-1]^* \setminus \operatorname{supp}(t_2) \subseteq \operatorname{supp}(t_1) \cap \operatorname{supp}(j)$, so there exist $2^{|\operatorname{supp}(t_1)\cap\operatorname{supp}(j)|} - 1$ such integers t_2. This observation shows that

$$\begin{aligned}|\{\rho_{t_1,t_2} \mid \rho_{t_1,t_2} \equiv 1 \pmod 2\}| \\ = \sum\big\{2^{|\operatorname{supp}(t_1)\cap\operatorname{supp}(j)|} - 1 \mid t_1 \in [k-1], [n-1]^* \setminus \operatorname{supp}(t_1) \subseteq \operatorname{supp}(i)\big\},\end{aligned}$$

https://doi.org/10.4153/S0008439519000365 Published online by Cambridge University Press

and hence

$$P_k^3(i,j) \equiv \sum\{2^{|\mathrm{supp}(t_1)\cap \mathrm{supp}(j)|}-1 \mid t_1 \in [k-1], [n-1]^* \setminus \mathrm{supp}(t_1) \subseteq \mathrm{supp}(i)\} \pmod 2.$$

Suppose that $i \neq j$. As $P_k^3(i,j)$ is congruent to an odd sum (namely, with $2^{|\mathrm{supp}(i)|}-1$ summands) of integers of the form $2^{|\mathrm{supp}(t_1)\cap\mathrm{supp}(j)|}-1$, it is sufficient to verify that $\mathrm{supp}(t_1)\cap\mathrm{supp}(j) \neq \varnothing$ for every $t_1 \in [k-1]$ that satisfies (i). Since $\overline{P_k^3}$ is symmetric, it can be assumed that $\mathrm{supp}(j) \setminus \mathrm{supp}(i) \neq \varnothing$ (because if $\mathrm{supp}(j)\setminus\mathrm{supp}(i) = \varnothing$, then $\mathrm{supp}(i)\setminus\mathrm{supp}(j) \neq \varnothing$, and hence the argument can be applied to the entry $P_k^3(j,i)$ instead). But $\mathrm{supp}(j)\setminus\mathrm{supp}(i) \subseteq [n-1]^*\setminus\mathrm{supp}(i) \subseteq \mathrm{supp}(t_1)$ by (i), so $\varnothing \neq \mathrm{supp}(j)\setminus\mathrm{supp}(i) \subseteq \mathrm{supp}(t_1)\cap\mathrm{supp}(j)$. Therefore, if $i \neq j$, then $P_k^3(i,j) \equiv 1 \pmod 2$.

Assume that $i = j$. The conditions $[n-1]^*\setminus\mathrm{supp}(t_1) \subseteq \mathrm{supp}(i)$ and $\mathrm{supp}(t_1)\cap\mathrm{supp}(i) = \mathrm{supp}(t_1)\cap\mathrm{supp}(j) = \varnothing$ hold if and only if $\mathrm{supp}(t_1)$ is the set-theoretic complement (in $[n-1]^*$) of $\mathrm{supp}(i)$, *i.e.*, if and only if $t_1 = k-i$. Hence, of the $2^{|\mathrm{supp}(i)|}-1$ integers $t_1 \in [k-1]$ that satisfy (i), there is exactly one such t_1 with $\mathrm{supp}(t_1)\cap\mathrm{supp}(j) = \varnothing$. Therefore, $P_k^3(i,i)$ is congruent to an even sum (namely, with $2^{|\mathrm{supp}(i)|}-2$ summands) of nonzero integers of the form $2^{|\mathrm{supp}(t_1)\cap\mathrm{supp}(j)|}-1$, and it follows that $P_k^3(i,i) \equiv 0 \pmod 2$. ∎

Let R be a finite Boolean ring. Since $|R| = 2^n$ for some $n \in \mathbb{N}$, every annihilator ideal of R has cardinality equal to a power of 2. In particular, every vertex of $\Gamma(R)$ has odd degree. Together with Theorem 3.1, this observation can now be used to provide an application of Boolean rings to determine the eigenvalues of the matrices $\overline{P_k}$ over $\overline{\mathbb{F}_2}$.

Theorem 3.4 *If $2 \le n \in \mathbb{N}$ and $k = 2^n - 1$, then the following statements hold.*

(i) *If $n = 2$, then $\overline{C_{P_k}} = X^2 + 1$.*

(ii) *If $n \ge 3$, then the minimal polynomial (over $\mathbb{F}_2$) of $\overline{P_k}$ is*

$$(X^3+1)(X+1) = X^4 + X^3 + X + 1.$$

In particular, the eigenvalue of $\overline{P_3}$ over $\overline{\mathbb{F}_2}$ is 1, and if $n \ge 3$, then the eigenvalues of $\overline{P_k}$ over $\overline{\mathbb{F}_2}$ are precisely the elements of $\mathbb{F}_4 \setminus \{0\}$ (neglecting multiplicities).

Proof The statement in (i) is clear. For (ii), let $M(X) \in \mathbb{F}_2[X]$ be the minimal polynomial of $\overline{P_k}$. Note that if $n \ge 3$, then every element of $\mathbb{F}_4\setminus\{0\}$ is an eigenvalue of $\overline{P_k}$ by (i), Corollary 3.2, and Proposition 2.2, and it follows that $(X+1)(X^2+X+1) = X^3+1$ divides $M(X)$ in $\mathbb{F}_2[X]$. Also, every vertex of $\Gamma(\mathbb{B}_{2^n})$ has odd degree, and thus $\overline{J_{k-1}P_k} = \overline{J_{k-1}}$ by Theorem 3.1. Hence, $\overline{(P_k^3 + I_{k-1})(P_k + I_{k-1})} = \overline{J_{k-1}(P_k - I_{k-1})}$ is the zero matrix (where the equality holds by Lemma 3.3), and therefore $M(X)$ divides $(X^3+1)(X+1)$ in $\mathbb{F}_2[X]$.

Since X^3+1 divides $M(X)$, and $M(X)$ divides $(X^3+1)(X+1)$, the result follows since $\overline{P_k^3 + I_{k-1}} = \overline{J_{k-1}}$ (a nonzero matrix) by Lemma 3.3. The "in particular" statement follows immediately by (i) and (ii). ∎

A finite simple graph Γ has a *perfect matching* if and only if there exists a permutation $\sigma \in S_{|V(\Gamma)|}$ with $\sigma = \sigma^{-1}$ such that $\prod_{i=1}^{|V(\Gamma)|} A(\Gamma)(i,\sigma(i)) \neq 0$. By noting that $A(\Gamma)(i,\sigma(i)) = A(\Gamma)(\sigma(i),i) = A(\Gamma)(\sigma(i),\sigma^{-1}(\sigma(i)))$, it follows that every

https://doi.org/10.4153/S0008439519000365 Published online by Cambridge University Press

permutation $\sigma \in S_{|V(\Gamma)|}$ satisfies $\prod_{i=1}^{|V(\Gamma)|} A(\Gamma)(i,\sigma(i)) = \prod_{i=1}^{|V(\Gamma)|} A(\Gamma)(i,\sigma^{-1}(i))$. Hence, if Γ has no perfect matching, then $\det(A(\Gamma))$ is a sum whose nonzero summands exist in pairs. In particular, if Γ has no perfect matching, then $\det(A(\Gamma)) \equiv 0 \pmod 2$ (*cf.* [5, Theorem 1.3]).

Let R be a commutative ring with identity such that $V(\Gamma(R)) \neq \varnothing$, and if $x, y \in V(\Gamma(R))$ have precisely the same adjacency relations, then $x = y$. By [9, Lemma 3.3], either R is a Boolean ring, $\Gamma(R)$ is a complete graph, or $\Gamma(R)$ does not have any perfect matchings. Indeed, if R is not a Boolean ring, then $Z(R)$ is an ideal with $r^2 = 0$ for every $r \in Z(R)$ ([11, Theorem 2.5]), and hence either $\Gamma(R)$ is complete or $Z(R)$ has even cardinality (*e.g.*, if x and y are nonadjacent vertices, then the equalities $2xy = (x+y)^2 = 0$ show that $\{0, xy\}$ is a subgroup of $Z(R)$). In the latter case, $|V(\Gamma(R))| = |Z(R)| - 1$ is odd, and therefore $\Gamma(R)$ does not have any perfect matchings.

The main result is now readily proved.

Corollary 3.5 *If R is a finite commutative ring with $1 \neq 0$, then R is a Boolean ring if and only if either $R \in \{\mathbb{F}_2, \mathbb{F}_2 \times \mathbb{F}_2\}$ or the eigenvalues in $\overline{\mathbb{F}_2}$ of $\Gamma(R)$ (neglecting multiplicities) are precisely the elements of $\mathbb{F}_4 \setminus \{0\}$.*

Proof The "only if" portion holds by Theorems 3.1 and 3.4. To prove the converse, note that if there exist distinct $x, y \in V(\Gamma(R))$ that have the same adjacency relations, then $\det(A(\Gamma(R)) = 0$ (*e.g.*, the rows of $A(\Gamma(R))$ corresponding to x and y are identical). Moreover, $\det(A(\Gamma(R)) \equiv 0 \pmod 2$ if $\Gamma(R)$ has no perfect matching (in particular, this is the case if $\Gamma(R)$ is a complete graph of odd order). Thus, in either case, it follows that 0 is an eigenvalue of $\Gamma(R)$ over $\overline{\mathbb{F}}_2$. Furthermore, as noted in the introduction, if $\Gamma(R)$ is a complete graph of even order, then 1 is the only eigenvalue of $\Gamma(R)$ over $\overline{\mathbb{F}_2}$. Therefore, by [9, Lemma 3.3], the hypotheses of the "if" statement imply that R is a Boolean ring. ∎

Let R be a finite commutative ring with $1 \neq 0$ and $V(\Gamma(R)) \neq \varnothing$. The proof of Corollary 3.5 yields a characterization of zero-divisor graphs whose only eigenvalue over $\overline{\mathbb{F}_2}$ is 1. Indeed, it shows that either 0 is an eigenvalue of $\Gamma(R)$ over $\overline{\mathbb{F}_2}$, $\Gamma(R)$ is a complete graph of even order, or R is Boolean, and it follows that 1 is the only eigenvalue of $\Gamma(R)$ over $\overline{\mathbb{F}_2}$ if and only if $\Gamma(R)$ is a complete graph of even order. By [1, Theorem 2.8], this holds if and only if either $R \cong \mathbb{F}_2 \times \mathbb{F}_2$, or $Z(R)$ is a nonzero ideal of odd cardinality such that $Z(R)^2 = \{0\}$. These observations are recorded in the next corollary.

Corollary 3.6 *The following statements are equivalent for a finite commutative ring R with $1 \neq 0$.*

(i) *1 is the only eigenvalue of $\Gamma(R)$ over $\overline{\mathbb{F}_2}$ (neglecting multiplicities).*
(ii) *$\Gamma(R)$ is a complete graph of even order.*
(iii) *$Z(R)$ is a nonzero ideal of odd cardinality such that $Z(R)^2 = \{0\}$.*

The investigation is closed with the following partial characterization of eigenvalues over $\overline{\mathbb{F}_2}$ of zero-divisor graphs of finite commutative rings, which holds by Corollary 3.5 and the discussion prior to Corollary 3.6.

https://doi.org/10.4153/S0008439519000365 Published online by Cambridge University Press

Corollary 3.7 *If R is a finite commutative ring with $1 \neq 0$, then at least one of the following statements holds:*

(i) *R is a field;*
(ii) *0 is an eigenvalue of $\Gamma(R)$ over $\overline{\mathbb{F}_2}$;*
(iii) *1 is the only eigenvalue of $\Gamma(R)$ over $\overline{\mathbb{F}_2}$ (neglecting multiplicities);*
(iv) *the eigenvalues of $\Gamma(R)$ over $\overline{\mathbb{F}_2}$ (neglecting multiplicities) are precisely the elements of $\mathbb{F}_4 \setminus \{0\}$.*

References

[1] D. F. Anderson and P. S. Livingston, *The zero-divisor graph of a commutative ring*. J. Algebra 217(1999), 434–447. https://doi.org/10.1006/jabr.1998.7840
[2] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*. Addison-Wesley, Reading, MA, 1969.
[3] S. Barik, M. Neumann, and S. Pati, *On nonsingular trees and a reciprocal eigenvalue property*. Linear Multilinear Algebra 54(2006), 453–465. https://doi.org/10.1080/03081080600792897
[4] L. Carlitz, *The characteristic polynomial of a certain matrix of binomial coefficients*. Fibonacci Quart. 3(1965), 81–89.
[5] D. M. Cvetković, M. Doob, and H. Sachs, *Spectra of graphs*. Theory and application. Pure and Applied Mathematics, 87, Academic Press, New York, 1979.
[6] N. J. Fine, *Binomial coefficients modulo a prime*. Amer. Math. Monthly 54(1947), 589–592. https://doi.org/10.2307/2304500
[7] C. Godsil and G. Royle, *Algebraic graph theory*. Graduate Texts in Mathematics, 207, Springer-Verlag, New York, 2001.
[8] J. D. LaGrange, *A combinatorial development of Fibonacci numbers in graph spectra*. Linear Algebra Appl. 438(2013), 4335–4347.
[9] J. D. LaGrange, *Boolean rings and reciprocal eigenvalue properties*. Linear Algebra Appl. 436(2012), 1863–1871. https://doi.org/10.1016/j.laa.2011.05.042
[10] J. D. LaGrange, *Eigenvalues of Boolean graphs and Pascal-type matrices*. Int. Electron. J. Algebra 13(2013), 109–119.
[11] D. Lu and T. Wu, *The zero-divisor graphs which are uniquely determined by neighborhoods*. Comm. Algebra 35(2007), 3855–3864. https://doi.org/10.1080/00927870701509156
[12] S. K. Panda and S. Pati, *On some graphs which satisfy reciprocal eigenvalue properties*. Linear Algebra Appl. 530(2017), 445–460. https://doi.org/10.1016/j.laa.2017.04.017

School of Mathematics and Sciences, Lindsey Wilson College, Columbia, KY 42728-1223, USA
e-mail: dillerys@lindsey.edu lagrangej@lindsey.edu

https://doi.org/10.4153/S0008439519000365 Published online by Cambridge University Press