INTEGER INVARIANTS OF ABELIAN CAYLEY GRAPHS

JOSHUA E. DUCEY AND DEELAN M. JALIL

Abstract. Let G be a finite abelian group, let E be a subset of G, and form the Cayley (directed) graph of G with connecting set E. We explain how, for various matrices associated to this graph, the spectrum can be used to give information on the Smith normal form. This technique is applied to several interesting examples, including matrices in the Bose-Mesner algebra of the Hamming association scheme $H(n, q)$. We also recover results of Bai and Jacobson-Niedermaier-Reiner on the critical group of a Cartesian product of complete graphs.

1. Introduction

Throughout this paper G will denote a finite abelian group (written multiplicatively) and E will denote a subset of G. We can then define a directed graph $\mathcal{C}$ with vertex set G, and an edge from h to g if and only if $gh^{-1} \in E$. We will refer to $\mathcal{C}$ as the Cayley graph of G with respect to the *connecting set* E. Note that $\mathcal{C}$ will be an undirected graph precisely when $E = E^{-1}$, where $E^{-1} = \{e^{-1} \,|\, e \in E\}$.

The purpose of this paper is to apply results of MacWilliams-Mann [12] and Sin [15] in order to obtain the Smith normal form of various matrices attached to many examples of these Cayley graphs. The structure of the paper is as follows. In the second section we explain basic terminology related to graphs and the Smith normal form of an integer matrix. In the third section we present and prove the results that motivate our computations. In the final section we apply these results to numerous examples.

2. Preliminaries

Generally speaking, when studying a graph one technique is to encode the information into a matrix, and then study certain numerical and algebraic properties of this matrix. Properties that remain the same up to isomorphism of graphs are called *invariants*. We now recall some popular matrices and invariants.

Ordering the vertices of a graph in some fixed (but arbitrary) manner, we can form the *adjacency matrix*, A, of the graph:

$$A(i, j) = \begin{cases} 1, & \text{if there is an edge from vertex } i \text{ to vertex } j \\ 0, & \text{otherwise,} \end{cases}$$

2010 *Mathematics Subject Classification.* 05C50.

Key words and phrases. Cayley graphs, invariant factors, elementary divisors, Smith normal form, Smith group, critical group, association schemes, adjacency matrix, Cartesian product of graphs, n-cube, Laplacian.

where the symbol $A(i,j)$ denotes the entry of the matrix A corresponding to row i and column j.

We can also consider the *Laplacian matrix*, L, defined by

$$L = D - A,$$

where D is the *degree matrix*:

$$D(i,j) = \begin{cases} \text{the (out) degree of vertex i}, & \text{if } i = j \\ 0, & \text{otherwise.} \end{cases}$$

The most well-known invariant of each of these associated matrices is the *spectrum*; that is, the eigenvalues and their multiplicities [4]. Even more fundamental is the *Smith normal form*, which can be defined more generally for (possibly nonsquare) incidence matrices. We say that two $m \times n$ integer matrices M and N are *equivalent*, and write

$$M \sim N,$$

if there exist integer matrices P and Q with determinants ± 1 so that

$$PMQ = N.$$

Such matrices P and Q are called *unimodular*, and the condition on their determinants simply forces their inverses to also be integer matrices.

It is well-known that each integer matrix M is equivalent to a matrix S such that

(1) $S(i,j) = 0$ if $i \neq j$, and
(2) $S(i,i)$ divides $S(i+1,i+1)$ for $1 \leq i < \min\{m,n\}$.

The matrix S is unique up to the sign of the $S(i,i)$ and is called the *Smith normal form* of M. The integers $S(i,i)$ are known as the *invariant factors* of the matrix M, for reasons we now explain. Viewing the matrix M as defining a homomorphism of free abelian groups

$$M\colon \mathbb{Z}^n \to \mathbb{Z}^m,$$

the cokernel $\mathbb{Z}^m/\operatorname{Im}(M)$ of this map has as its invariant factor decomposition [6, Chap. 12, Theorem 5]

$$\prod \mathbb{Z}/S(i,i)\mathbb{Z}.$$

We can further decompose this cokernel into cyclic groups of prime power order–its elementary divisor decomposition–and for this reason the prime power factors of the invariant factors of M are known as the *elementary divisors* of M. The purpose of going through this terminology is to stress that when one tries to find the Smith normal form of an integer matrix, one is really seeking a description of this cokernel, and this is a problem that can be solved one prime at a time.

Returning now to graphs, we remark that when we are looking at the adjacency matrix this cokernel goes by the name of the *Smith group* of the graph [13]. The torsion subgroup of the Laplacian cokernel has many names in the literature [11], one of which is the *critical group* of the graph. The critical group of a graph is especially interesting because it has geometric and combinatorial interpretations: the order of the critical group is the number of spanning forests in the graph, a connected graph is a tree if and only if its Laplacian is 'unimodularly congruent' to its Smith normal form [10], etc.

3. Eigenvalues as Character Sums

We return to the situation described in the introduction. Thus G is a finite abelian group, E is a subset of G, and $\mathcal{C}$ is the corresponding Cayley graph. Denote by A_E the adjacency matrix of this graph.

In what follows we will require some basic familiarity with characters. Most of what we need can be found in, for example, [7, Chaps. 2 and 3]. The following is a well-known result expressing the eigenvalues of A_E in terms of the irreducible complex characters of G, and was first observed in [12]. For completeness we provide a short proof.

Theorem 3.1. *Let* $\mathrm{Irred}(G)$ *denote the set of irreducible complex characters of G. Let M denote the character table of G, with rows indexed by* $\mathrm{Irred}(G)$ *and columns indexed by G in the same order as for A_E. Then*

$$\frac{1}{|G|} M A_E^t \overline{M}^t = \mathrm{diag}\left(\sum_{e\in E}\chi(e)\right)_{\chi\in\mathrm{Irred}(G)}. \tag{3.1}$$

Thus the eigenvalues of A_E take the form $\sum_{e\in E}\chi(e)$, for $\chi \in$ $\mathrm{Irred}(G)$.

Proof. Observe that

$$\begin{aligned} MA_E^t(\chi, g) &= \sum_{\substack{h\in G\\ hg^{-1}\in E}} \chi(h) \\ &= \sum_{e\in E}\chi(eg). \end{aligned}$$

Thus we have

$$\begin{aligned} MA_E^t\overline{M}^t(\chi,\psi) &= \sum_{g\in G}\sum_{e\in E}\chi(eg)\overline{\psi(g)} \\ &= \sum_{e\in E}\chi(e)\cdot\sum_{g\in G}\chi(g)\overline{\psi(g)} \\ &= \begin{cases} |G|\sum_{e\in E}\chi(e), & \text{if } \chi=\psi \\ 0, & \text{otherwise} \end{cases} \end{aligned}$$

where the last equality follows from the orthogonality relations. This proves equation (3.1). Again by the orthogonality relations we have that $\frac{1}{|G|}M\overline{M}^t = I$; from this the final statement follows. □

Thus finding the spectrum of A_E is reduced to computing the character sums $\sum_{e\in E}\chi(e)$. Generally speaking, the spectrum of an integer matrix has little connection to its elementary divisors. See [14, 15] for a discussion in the context of the adjacency matrix, and [11] for what can be said about the Laplacian. For abelian Cayley graphs the connection to the Smith normal form of A_E is made by an important observation of Sin [15, p. 1364], which we paraphrase in the following two theorems.

Observe that since A_E is a zero-one matrix, we can view its entries as coming from any commutative ring. In what follows K will denote an algebraic closure of the field of p-adic numbers, $\mathbb{Q}_p$. We let $\zeta \in K$ denote a primitive $|G|$-th root of unity. The ring of p-adic integers is denoted $\mathbb{Z}_p$ and we set $R = \mathbb{Z}_p[\zeta]$. Recall that a prime element $\pi \in R$ is said to *lie over* the prime $p \in \mathbb{Z}_p$ if $\pi R \cap \mathbb{Z}_p = p\mathbb{Z}_p$.

Theorem 3.2. *Let p be a prime integer that does not divide $|G|$, let i be a positive integer. Let $\pi \in R$ be a prime lying over $p \in \mathbb{Z}_p$. Then the multiplicity of p^i as an elementary divisor of A_E is equal to the number of eigenvalues of A_E exactly divisible by π^i in R.*

Proof. Our preliminary facts and terminology about the Smith normal form carry over with very slight modification when one replaces the integers with any principal ideal domain. It is clear that the multiplicity of p^i as an elementary divisor of A_E remains the same when one views the matrix entries as coming from the ring of p-adic integers $\mathbb{Z}_p$. Now let ζ be a primitive $|G|$-th root of unity in an algebraic closure K of the field of p-adic numbers, $\mathbb{Q}_p$, and consider the ring $R = \mathbb{Z}_p[\zeta]$. The prime p is unramified in the extension $\mathbb{Z}_p \subset R$ since $p \nmid |G|$, hence the multiplicity of p^i as an elementary divisor of A_E over $\mathbb{Z}_p$ is the same as the multiplicity of π^i as an elementary divisor of A_E over R for any prime π of R lying over p. Since $\overline{M}(\chi, g) = M(\chi, g^{-1})$, the matrices in Theorem 3.1 can be viewed as having entries from R, and since $\frac{1}{|G|}M\overline{M}^t = I$ we see that equation (3.1) defines an equivalence of matrices over R. The theorem follows. □

Remarks.

(1) It is obvious that the conclusion of Theorem 3.2 remains true if we replace A_E by any matrix diagonalized by M. This includes linear combinations of the A_E and the identity matrix; in particular, the Laplacian, signless Laplacian, Seidel adjacency matrix, etc.
(2) See an example in Section 4.5 below of when A_E has non-integer eigenvalues. However, the most common situation we will encounter is when all of the eigenvalues of A_E are integers. In this case we have the following useful result.

Theorem 3.3. *Let p be a prime integer that does not divide $|G|$, let i be a positive integer. Suppose that the eigenvalues of A_E are all integers. Then the multiplicity of p^i as an elementary divisor of A_E is the same as the number of eigenvalues of A_E exactly divisible by p^i.*

Proof. An integer not divisible by p becomes a unit in $\mathbb{Z}_p$, hence will also not be divisible by any $\pi \in R$ lying over $p \in \mathbb{Z}_p$. The result now follows from Theorem 3.2. □

We now apply these theorems in conjunction to obtain strong results about elementary divisors for a variety of examples.

4. Applications

Since G is a finite abelian group, it is isomorphic to a direct product of cyclic groups. We will form interesting Cayley graphs by using a fixed cyclic decomposition of G to define our connecting set. One construction will be used so often that we define it now. Under the identification

$$G = Z_{q_1} \times Z_{q_2} \times \cdots \times Z_{q_n},$$

where Z_q denotes the (multiplicative) cyclic group of order q, define the connecting sets E_k, for $0 \leq k \leq n$:

$$E_k \coloneqq \{g \in G \,|\, \text{exactly } k \text{ components of } g \text{ are not equal to the identity}\}.$$

When we are dealing with a Cayley graph defined by a connecting set E_k, we will write A_k instead of A_{E_k} for the adjacency matrix. We denote by $[n]$ the set $\{1, 2, \ldots, n\}$ and we denote by $\binom{[n]}{k}$ the collection of subsets of $[n]$ of size k.

We can provide a reasonable description of the eigenvalues $\sum_{e \in E_k} \chi(e)$ of A_k. Let $\chi \in \mathrm{Irred}(G)$. Then, for $g = (g_1, g_2, \ldots, g_n) \in G$, χ takes the form

$$\chi(g) = \chi_1(g_1)\chi_2(g_2)\cdots\chi_n(g_n)$$

for some $\chi_i \in \mathrm{Irred}(Z_{q_i})$.

We have that

$$\begin{aligned} \sum_{e \in E_k} \chi(e) &= \sum_{(e_1, e_2, \ldots, e_n) \in E_k} \chi_1(e_1)\chi_2(e_2)\cdots\chi_n(e_n) \\ &= \sum_{K \in \binom{[n]}{k}} \prod_{i \in K} \sum_{\substack{e_i \in Z_{q_i} \\ e_i \neq 1}} \chi_i(e_i) \end{aligned} \tag{4.1}$$

and by considering the inner product of χ_i with the principal character of Z_{q_i} we see that

$$\sum_{\substack{e_i \in Z_{q_i} \\ e_i \neq 1}} \chi_i(e_i) = \begin{cases} q_i - 1, & \text{if } \chi_i \text{ is principal} \\ -1, & \text{otherwise.} \end{cases}$$

4.1. **The Hamming association scheme.** Let $H(n, q)$ denote the Hamming association scheme; that is, $H(n, q)$ consists of n-tuples with coordinates coming from an alphabet of size q. Two such tuples are k-th associates if they differ in exactly k coordinate positions. Setting $G = Z_q \times Z_q \times \cdots \times Z_q$ (n times), we see that the distance k association matrix of $H(n, q)$ is precisely A_k. We remark again that our approach applies not just to the adjacency matrices but to any matrix in the Bose-Mesner algebra [5, p. 9] of $H(n, q)$.

In this case the value of (4.1) depends only on the number of χ_i that are principal. Explicitly, if exactly ℓ of the χ_i are principal, (4.1) collapses to express the eigenvalues in their usual form as integer values of the Krawtchouk polynomials [5, p. 38]:

$$\sum_{(e_1, e_2, \cdots, e_n) \in E_k} \chi_1(e_1)\chi_2(e_2)\cdots\chi_n(e_n) = \sum_{j=0}^{k} \binom{\ell}{j}\binom{n-\ell}{k-j}(q-1)^j(-1)^{k-j}. \tag{4.2}$$

The number of $\chi \in \mathrm{Irred}(G)$ consisting of exactly ℓ copies of the principal character of Z_q is $\binom{n}{\ell}(q-1)^{n-\ell}$, and we can apply Theorem 3.3 to (4.2) to compute the p-elementary divisor multiplicities of A_k, for primes p not dividing q.

It is often the case that many of the terms in (4.2) are equal to zero. In particular, consider the maximal distance association matrix A_n. From (4.2) we see that the eigenvalues of A_n are $(q-1)^\ell(-1)^{n-\ell}$ occurring with multiplicity $\binom{n}{\ell}(q-1)^{n-\ell}$. Since a prime that divides q will not divide $q - 1$, we see that all of the elementary divisors of A_n can be obtained from the spectrum in this case; and, in fact, the invariant factors of A_n are *equal* to its eigenvalues. This fact was conjectured in [2] and first proved in [15].

If we restrict ourselves to the binary Hamming scheme $H(n, 2)$, then the situation becomes simpler. The association matrices A_k and A_{n-k} are the same up to row permutation, hence they share the same Smith normal form. The distance 1 matrix is then the adjacency matrix for the well-studied n-cube graph.

4.2. **The n-cube graph.** Here $G = Z_2 \times Z_2 \times \cdots \times Z_2$ (n times), $E = E_1$, and $A = A_1$ is the adjacency matrix of the n-cube graph. Thus Theorem 3.3 applies to give us the p-elementary divisors of A for odd primes p. Here (4.2) collapses to give us eigenvalues

$$-n + 2\ell \tag{4.3}$$

occurring with multiplicity $\binom{n}{\ell}$, for $0 \leq \ell \leq n$. These eigenvalues have come up in many applications [17, Chap. 7], [16]. We see that when n is odd, all of the eigenvalues of A are odd (and A is nonsingular). Thus A has only odd elementary divisors and so the complete structure of the Smith group of the n-cube can be deduced from the eigenvalues in this case. When n is even, however, the 2-primary component of the Smith group will be nontrivial. We will return to the 2-part of A in our discussion of Laplacians below.

4.3. **Cartesian products of complete graphs.** Generalizing the n-cube graph we now set $G = Z_{q_1} \times Z_{q_2} \times \cdots \times Z_{q_n}$ but continue to use connecting set $E = E_1$. We again write $A = A_1$ for the adjacency matrix. Cayley graphs of this form are precisely the Cartesian products of complete graphs.

To describe the eigenvalues corresponding to $\chi = (\chi_1, \chi_2, \cdots, \chi_n) \in \mathrm{Irred}(G)$, we need to know not just how many of the χ_i are principal but their locations as well. Say $\chi_{i_1}, \chi_{i_2}, \cdots, \chi_{i_\ell}$ are the principal ones. Then (4.1) simplifies to

$$-n + \sum_{j=1}^{\ell} q_{i_j} \tag{4.4}$$

and there are $\prod_{i \notin \{i_1, i_2, \cdots, i_\ell\}} (q_i - 1)$ characters $\chi \in \mathrm{Irred}(G)$ of this form. From this we can deduce the p-elementary divisors of A for primes p that divide none of the q_i, $0 \leq i \leq n$.

4.4. **The Laplacian and the critical group.** As the Cayley graph is regular with valency $|E|$, the adjacency spectrum determines the Laplacian spectrum. We now recover some powerful results on the critical group of some of the Cayley graphs above.

4.4.1. *The critical group of the n-cube.* Let L denote the Laplacian matrix of the n-cube. Then equation (4.3) implies that the eigenvalues of L are 2ℓ occurring with multiplicity $\binom{n}{\ell}$, for $0 \leq \ell \leq n$. It follows that, for odd primes p, the Sylow p-subgroup of the critical group of the n-cube is isomorphic to

$$\prod_{\ell=1}^{n} Syl_p(Z_\ell)^{\binom{n}{\ell}}. \tag{4.5}$$

This is the main result of [1].

In general, the full structure of the 2-primary component of both the critical group and the Smith group of the n-cube remain unknown. In [1, Theorem 1.3],the 2-rank of L is shown to be equal to 2^{n-1}, and the multiplicity of 2 as an elementary divisor of L is also determined. As we mentioned earlier, for odd n the 2-rank of the adjacency matrix A is 2^n. For even n, note that by definition of the Laplacian we have that $L \equiv A \pmod 2$. Hence, for even n, the 2-rank of A is also 2^{n-1}. More generally, if $L \equiv A \pmod{2^i}$ then the multiplicity of 2^j, $0 \leq j < i$, as an elementary divisor is the same for both A and L [3, Lemma 3.3]. Computer calculations seem to indicate that the 2-primary component of the Smith group may be easier to understand. We conjecture that the multiplicity of 2^i as an elementary divisor of A is equal to the number of eigenvalues of A exactly divisible by 2^{i+1}.

4.4.2. *The critical group of a Cartesian product of complete graphs.* The previous result on the p-primary component of the critical group of the n-cube, for odd primes p, was generalized to the critical group of a Cartesian product of complete graphs [8, Theorem 1.2].Recall that such a graph is the Cayley graph $\mathcal{C}$ of $G = Z_{q_1} \times Z_{q_2} \times \cdots \times Z_{q_n}$ with connecting set $E = E_1$. Let $A = A_1$ denote the adjacency matrix and let L denote the Laplacian. From equation (4.4) we deduce that each subset $\{i_1, i_2, \cdots, i_\ell\}$ of $[n]$ determines $\prod_{i \notin \{i_1, i_2, \cdots, i_\ell\}} (q_i - 1)$ eigenvalues of L of the form

$$n - \sum_{j=1}^{\ell} q_{i_j} + \sum_{i=1}^{n} (q_i - 1) = \sum_{i \notin \{i_1, i_2, \cdots, i_\ell\}} q_i.$$

It follows that, for a prime p not dividing any of the q_i, $1 \leq i \leq n$, the Sylow p-subgroup of the critical group of $\mathcal{C}$ is isomorphic to

$$\prod_{\substack{S \subseteq [n] \\ S \neq [n]}} Syl_p(Z_{\sum_{i \notin S} q_i})^{\prod_{i \notin S}(q_i - 1)}.$$

This result was proved in [8]. It is worth mentioning that the proof in [8] relies heavily on keeping track of integral row and column operations on L. Our proof of (4.5) is also of a very different nature than the proof in [1].

4.5. **Non-integer eigenvalues.** It was observed in [9, Example 4.1] that if we take our connecting set E to be any union of the E_i then the eigenvalues of A_E are all integers. We conclude with a small non-integer example.

Let $G = Z_7 = \langle x \rangle$ and use connecting set $E = \{x^4, x^5, x^6\}$. Following the notation preceding Theorem 3.2, $\zeta \in K$ is a primitive 7-th root of unity and set $\alpha = \zeta^5 + \zeta^2 + \zeta + 1$ and $\beta = \zeta^5 + \zeta^4 + \zeta^3 + 1$. Notice that in the ring $R = \mathbb{Z}_2[\zeta]$ we have $2 = \zeta^2 \cdot \alpha \cdot \beta$. The adjacency matrix A_E has seven distinct eigenvalues:

$$3, \quad -\alpha, \quad -\zeta^2\alpha, \quad -\zeta^3\beta, \quad -\zeta^6\alpha, \quad -\beta, \quad -\zeta^2\beta.$$

From Theorem 3.2 we deduce that 3 is an elementary divisor of A_E with multiplicity 1 and 2 is an elementary divisor of A_E with multiplicity 3.

5. Acknowledgements

This work was supported by the James Madison University Program of Grants for Faculty Assistance. The authors also acknowledge helpful comments from Peter Sin, Dino Lorenzini, and the anonymous referee.

References

[1] Hua Bai. On the critical group of the n-cube. *Linear Algebra Appl.*, 369:251–261, 2003.

[2] Stephanie Bittner, Xuyi Guo, and Adam Zweber. Approaches to Rota's basis conjecture. *Report on James Madison University Summer REU*, 2012.

[3] Andries E. Brouwer, Joshua E. Ducey, and Peter Sin. The elementary divisors of the incidence matrix of skew lines in $PG(3, q)$. *Proc. Amer. Math. Soc.*, 140(8):2561–2573, 2012.

[4] Andries E. Brouwer and Willem H. Haemers. *Spectra of graphs*. Universitext. Springer, New York, 2012.

[5] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97, 1973.

[6] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[7] I. Martin Isaacs. *Character theory of finite groups*. AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423].

[8] Brian Jacobson, Andrew Niedermaier, and Victor Reiner. Critical groups for complete multipartite graphs and Cartesian products of complete graphs. *J. Graph Theory*, 44(3):231–250, 2003.

[9] Walter Klotz and Torsten Sander. Integral Cayley graphs over abelian groups. *Electron. J. Combin.*, 17(1):Research Paper 81, 13, 2010.

[10] Hao Liang, Yong-Liang Pan, Jian Wang, and Jun-Ming Xu. A note on unimodular congruence of the Laplacian matrix of a graph. *Linear Multilinear Algebra*, 58(3-4):497–501, 2010.

[11] Dino Lorenzini. Smith normal form and Laplacians. *J. Combin. Theory Ser. B*, 98(6):1271–1300, 2008.

[12] F. J. MacWilliams and H. B. Mann. On the p-rank of the design matrix of a difference set. *Information and Control*, 12:474–488, 1968.

[13] Joseph J. Rushanan. Combinatorial applications of the Smith normal form. In *Proceedings of the Twentieth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1989)*, volume 73, pages 249–254, 1990.

[14] Joseph J. Rushanan. Eigenvalues and the Smith normal form. *Linear Algebra Appl.*, 216:177–184, 1995.

[15] Peter Sin. Smith normal forms of incidence matrices. *Sci. China Math.*, 56(7):1359–1371, 2013.

[16] Richard P. Stanley. Cubes and the radon transform. In *Algebraic Combinatorics: Walks, Trees, Tableaux, and More*, Undergraduate Texts in Mathematics. Springer New York, 2013.

[17] J. H. van Lint. *Introduction to coding theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 1999.

Dept. of Mathematics and Statistics, James Madison University, Harrisonburg, VA 22807

E-mail address: duceyje@jmu.edu

Dept. of Mathematics and Statistics, James Madison University, Harrisonburg, VA 22807

E-mail address: jalil2dm@jmu.edu