Integral Cayley graphs over a finite symmetric algebra

Tung T. Nguyen and Nguyen Duy Tan

Lake Forest College

The 2025 annual Meeting of the Illinois Section of the MAA

What is a graph?

A (undirected) graph is an ordered pair $G = (V, E)$ where

- V is a finite set whose elements are called vertices,
- E is a set of paired vertices.

Suppose the vertex set of G is $\{v_1, v_2, \ldots, v_n\}$. A convenient way to represent G is to use its adjacency matrix $\boldsymbol{A} = (a_{ij})$ where

$$a_{ij} = \begin{cases} 1 & \text{if } (v_i, v_j) \in E \\ 0 & \text{else.} \end{cases}$$

With this presentation, we can then use tools from matrix theory, representation theory, and number theory to study the structure of G.

Example 1: Complete graph

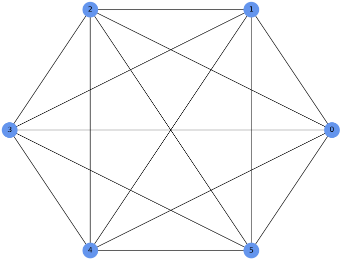

Figure 1: The complete graph K_6 on $n = 6$ nodes

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

The adjacency matrix of K_6

Another example: An Erdős–Rényi random graph

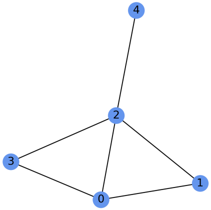

Figure 2: A random graph on $n = 5$ nodes

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

The adjacency matrix of this graph.

Graph spectra

- The spectrum of G, denoted by $\text{Spec}(G)$, is the set of all eigenvalues of its adjacency matrix A. Equivalently, it is the set of all roots of the characteristic polynomial $p_A(t)$ of A where
$$p_A(t) = \det(tI_n - A).$$
- A graph is called integral if $\lambda \in \mathbb{Z}$ for each $\lambda \in \text{Spec}(G)$.

A concrete example

Let us consider the spectrum of the complete graph K_3 on three nodes. Its adjacency matrix is given by

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

The characteristic polynomial of A is given by

$$p_A(t) = \det(tI_3 - A) = \begin{vmatrix} t & -1 & -1 \\ -1 & t & -1 \\ -1 & -1 & t \end{vmatrix} = t^3 - 3t - 2 = (t-2)(t+1)^2.$$

Therefore, the spectrum of K_3 is $\{[2]_1, [-1]_2\}$.

In general, the spectrum of K_n is $\{[n-1]_1, [-1]_{n-1}\}$. This shows that K_n is an integral graph for all n.

Circulant graphs

In general, the classification of integral graphs is a difficult problem. However, for certain arithmetic graphs, this problem is more tractable.

Definition

A graph G is called circulant if it is equiped with the following data

- $V(G) = \mathbb{Z}/n = \{0, 1, \ldots, n-1\}$
- *There exists a subset $S \subset \mathbb{Z}/n$ such that $a, b \in V(G)$ are adjacent if $a - b \pmod{n}$ is an element of S.*

For example, if $S = \{1, 2, \ldots, n-1\}$ then G is precisely the complete graph K_n.

The Circulant Diagonalization Theorem

Let G be a circulant graph with $n = 3$. The adjacency matrix of G is a 3×3 matrix of the form

$$C = \begin{pmatrix} c_0 & c_1 & c_2 \\ c_2 & c_0 & c_1 \\ c_1 & c_2 & c_0 \end{pmatrix}.$$

Let ω_3 be 3-root of unity; namely $\omega_3^3 = 1$. Then we have

$$C \begin{pmatrix} 1 \\ \omega_3 \\ \omega_3^2 \end{pmatrix} = \begin{pmatrix} c_0 + c_1\omega_3 + c_2\omega_3^2 \\ c_2 + c_0\omega_3 + c_1\omega_3^2 \\ c_1 + c_2\omega_3 + c_0\omega_3^2 \end{pmatrix} = \begin{pmatrix} (c_0 + c_1\omega_3 + c_2\omega_3^2)1 \\ (c_0 + c_1\omega_3 + c_2\omega_3^2)\omega_3 \\ (c_0 + c_1\omega_3 + c_2\omega_3^2)\omega_3^2 \end{pmatrix}.$$

We see that $(1, \omega_3, \omega_3^2)^t$ is an eigenvector of C associated with the eigenvalue $c_0 + c_1\omega_3 + c_2\omega_3^2$.

More generally we have the following theorem.

Theorem

Let G be a circulant graph associated with a subset $S \subset \mathbb{Z}/n$. Let $\vec{c} = (c_0, c_1, \ldots, c_{n-1})$ be the first row vector of A_G. Let

$$v_{n,j} = \frac{1}{\sqrt{n}} \left(1, \omega_n^j, \omega_n^{2j}, \ldots, \omega_n^{(n-1)j}\right)^T, \quad j = 0, 1, \ldots, n-1.$$

Then $v_{n,j}$ is an eigenvector of C associated with the eigenvalue

$$\lambda_j = c_0 + c_1\omega_n^j + c_2\omega_n^{2j} + \cdots + c_{n-1}\omega_n^{(n-1)j} = \sum_{i \in S} \omega_n^{ij}.$$

In other words, the spectrum of G is precisely the Discrete Fourier Transform of $\vec{c}$.

- By the CDT theorem, a circulant graph G is integral if $\lambda_j \in \mathbb{Z}$ for all $0 \leq j \leq n-1$. By Galois theory, this occurs if $\sigma(\lambda_j) = \lambda_j$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$.
- The Galois group $\mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/n)^\times$. In fact, each $a \in (\mathbb{Z}/n)^\times$ produces $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$ defined by $\sigma_a(\omega_n) = \omega_n^a$.
- By definition
$$\sigma_a(\lambda_j) = \sum_{i \in S} \omega_n^{aij} = \sum_{i \in aS} \lambda_n^{ij}$$
- We conclude that if $aS = S$ for all $a \in (\mathbb{Z}/n)^\times$ then $\sigma_a(\lambda_j) = \lambda_j$. In other words, G is integral.

What is a gcd-graph?

- We say that a circulant graph G is a gcd-graph if the generating set S has the property that $aS = S$ for all $a \in (\mathbb{Z}/n)^{\times}$. In other words, if $d \in S$ then $ad \in S$ for all $a \in (\mathbb{Z}/n)^{\times}$.
- We can show that if G is a gcd-graph, then there exists a subset $D = \{d_1, d_2, \ldots, d_k\}$ of proper divisors of n with the property that: for each $s \in \mathbb{Z}/n$, $s \in S$ if and only if $\gcd(s, n) \in D$.

An example

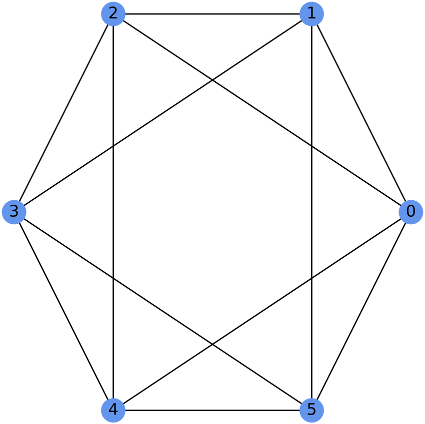

Figure 3: The gcd-graph $G_n(D)$ with $n = 6$ and $D = \{1, 2\}$

Gcd-graphs are integral

The above Galois-theoretic argument described above shows that a gcd-graph is necessarily integral.

Question

Is the converse true? In other words, if G is integral, is it true that G is a gcd-graph?

Gcd-graphs are integral

The above Galois-theoretic argument described above shows that a gcd-graph is necessarily integral.

Question

Is the converse true? In other words, if G is integral, is it true that G is a gcd-graph?

Answer (So's theorem)

If a circulant graph G is integral, it must be a gcd-graph with respect to some choice of D.

A few remarks about gcd-graphs

- Gcd-graphs were introduced by Klotz and Sander as a generalization of unitary Cayley graphs (corresponding to the case $D = \{1\}$).
- Using the theory of Ramanujuan sums, they are able to describe explicitly the spectrum of $G_n(D)$. More specifically, its spectrum is $(\lambda_m)_{m \in \mathbb{Z}/n}$ where

$$\boxed{\lambda_m = \sum_{d \in D} c(m, n/d),}$$

and

$$\boxed{c(m, n/d) = \mu(t) \frac{\varphi(n/d)}{\varphi(t)}, \quad \text{where} \quad t = \frac{n/d}{\gcd(n/d, m)}.}$$

- This description gives a more explicit proof that gcd-graphs are integral graphs.

Integral graphs over a finite commutative ring

Let R be a finite commutative ring and S a subset of R. Let $G = \Gamma(R, S)$ be the graph with the following data

- The vertex set of G is R.
- Two vertices a, b of G are adjacent if $a - b \in S$.

Question

Can we classify S such that $G = \Gamma(R, S)$ is integral?

By the same argument, we can show that if S has the property that $aS = S$ for each $a \in (\mathbb{Z}/n)^\times$ where n is the characteristic of R, then $\Gamma(R, S)$ is integral.

Main Theorem

Theorem (Nguyen-Tan, 2025)

Let R be a finite symmetric $\mathbb{Z}/n$-algebra. Then graph $\Gamma(R, S)$ is integral if and only if $aS = S$ for each $a \in (\mathbb{Z}/n)^{\times}$.

- The definition of a symmetric algebra is a bit complicated. Roughly, speaking its is an algebra where the dual group $\text{Hom}(R, \mathbb{C}^{\times})$ is isomorphic to R.
- Similar to the case where $R = \mathbb{Z}/n$, we can explicitly calculate the spectrum of $\Gamma(R, S)$ using the theory of generalized Ramanujan sums that were developed in the 50s by Lamprecht.

Acknowledgements

We gratefully acknowledge the following organizations for their support:

- Lake Forest College for their support with an Overleaf subscription.
- AMS-Simons Travel Grant
- Vietnam National Foundation for Science and Technology Development (NAFOSTED)

Thank You!