On Gcd Graphs over Polynomial Rings

Ján Mináč, Tung T. Nguyen, and Nguyen Duy Tan

Lake Forest College

2025 SIAM Conference on Applied Algebraic Geometry
July 2025, Madison, Wisconsin

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 $A = A_G = (a_{ij})$ 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.

An Erdős–Rényi random graph

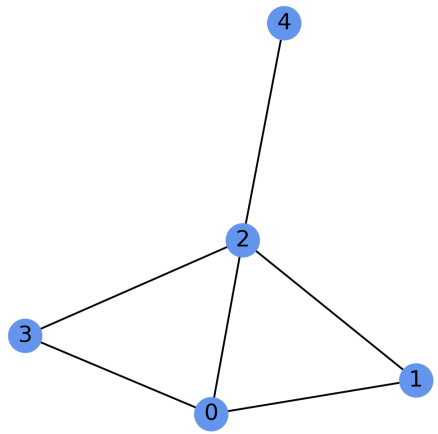

Figure 1: A random graph on $n = 5$ nodes

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

The adjacency matrix of this graph.

Graph spectra

- The spectrum of G, denoted by $\mathrm{Spec}(G)$, 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
$$p_A(t) = \det(tI_n - A).$$
- Let K be a subfield of $\mathbb{C}$. A graph is called K-rational if $\lambda \in \mathcal{O}_K$ for each $\lambda \in \mathrm{Spec}(G)$ where $\mathcal{O}_K$ is the ring of integers in K.
- A $\mathbb{Q}$-rational graph is often called an integral graph.

Perfect state transfer on graphs

Definition

Let $F(t)$ be the continuous-time quantum walk associated with G; namely $F(t) = \exp(\mathrm{i}A_G t)$. There is perfect state transfer (PST) in graph G if there are distinct vertices a and b and a positive real number t such that $|F(t)_{ab}| = 1$.

Perfect state transfer on graphs

Definition

Let $F(t)$ be the continuous-time quantum walk associated with G; namely $F(t) = \exp(\mathrm{i}A_G t)$. There is perfect state transfer (PST) in graph G if there are distinct vertices a and b and a positive real number t such that $|F(t)_{ab}| = 1$.

The adjacency matrix of K_2 is

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

Definition

Let $F(t)$ be the continuous-time quantum walk associated with G; namely $F(t) = \exp(\mathrm{i}A_G t)$. There is perfect state transfer (PST) in graph G if there are distinct vertices a and b and a positive real number t such that $|F(t)_{ab}| = 1$.

The adjacency matrix of K_2 is

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

$$F(t) = \cos(t)I + \mathrm{i}\sin(t)A = \begin{bmatrix} \cos(t) & \mathrm{i}\sin(t) \\ \mathrm{i}\sin(t) & \cos(t) \end{bmatrix}.$$

and hence

$$F\left(\frac{\pi}{2}\right) = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

This shows that there is PST between u and v at $t = \frac{\pi}{2}$.

Theorem (Godsil)

Suppose that there is PST on G.

1. *G is K-rational where K is either $\mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$.*
2. *If G is regular, then it is $\mathbb{Q}$-rational.*

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 $\mathbb{Z}/n$-circulant if it is equipped 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.*

We will write $G = \Gamma(\mathbb{Z}/n, S)$.

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 $c_0 + c_1\omega_3 + c_2\omega_3^2$.

The Circulant Diagonalization Theorem

More generally we have the following theorem.

Theorem (Circulant Diagonalization 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 ζ_n be a fixed primitive n-root of unity and

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

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

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

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

Integral Circulant Graphs

- 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 $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.
- The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/n)^\times$. In fact, each $a \in (\mathbb{Z}/n)^\times$ produces $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ defined by $\sigma_a(\zeta_n) = \zeta_n^a$.
- By definition
$$\sigma_a(\lambda_j) = \sum_{i \in S} \zeta_n^{aij} = \sum_{i \in aS} \lambda_n^{ij}$$
- 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.

Question

Is the converse true? In other words, if $\Gamma(\mathbb{Z}/n, S)$ is integral, is it true that S is stable under the action of $(\mathbb{Z}/n)^\times$?

Question

Is the converse true? In other words, if $\Gamma(\mathbb{Z}/n, S)$ is integral, is it true that S is stable under the action of $(\mathbb{Z}/n)^\times$?

Answer (So's theorem)

Yes. If a circulant graph G is integral, then S is stable under the action of $(\mathbb{Z}/n)^\times$.

Question

Is the converse true? In other words, if $\Gamma(\mathbb{Z}/n, S)$ is integral, is it true that S is stable under the action of $(\mathbb{Z}/n)^\times$?

Answer (So's theorem)

Yes. If a circulant graph G is integral, then S is stable under the action of $(\mathbb{Z}/n)^\times$.

We can show that S is stable under the action of $(\mathbb{Z}/n)^\times$ if and only if 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 $\gcd(s, n) \in D$. Such a graph is called a gcd-graph over $\mathbb{Z}$.

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?

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?

Definition

A finite $\mathbb{Z}/n$-algebra R is called Frobenius ring if there exists a linear functional $\psi : R \to \mathbb{Z}/n$ such that the kernel of ψ does not contain any non-zero ideal in R.

Examples

- $R = \mathbb{Z}/n$. In this case, the identity function $\mathbb{Z}/n \to \mathbb{Z}/n$ is a non-degenerate linear form.
- $R = \mathbb{F}_p[x]/f$ where $f = \sum_{i=0} a_i x^i$ is a non-constant polynomial. Every element of R can be written in the form $g = \sum_{i=0}^{m-1} b_i x^i$. In this case, the function $\psi : R \to \mathbb{F}_p$ defined by

  $$\psi(g) = b_{m-1}$$

  is a non-degenerate linear functional on R.
- More generally, we can show that if K is a global field then any finite quotient of $\mathcal{O}_K$ is a Frobenius ring.
- R is a Frobenius ring, then $R[G]$ is also a Frobenius ring where G is a finite abelian group.

A key property of a finite Frobenius ring is that the characters of $(R, +)$ are precisely $\chi_r = \zeta_n^{\psi_r}$ where $\psi_r(a) = \psi(ra)$. In other words, the dual group $\mathrm{Hom}(R, \mathbb{C}^\times)$ is a cyclic R-module.

A key property of a finite Frobenius ring is that the characters of $(R,+)$ are precisely $\chi_r = \zeta_n^{\psi_r}$ where $\psi_r(a) = \psi(ra)$. In other words, the dual group $\mathrm{Hom}(R, \mathbb{C}^\times)$ is a cyclic R-module.

Theorem (Nguyen-Tan)

Let R be a finite Frobenius ring with characteristic n. Let K be a subfield of $\mathbb{Q}(\zeta_n)$. Then the graph $\Gamma(R,S)$ is K-rational if and only if S is stable under the action of H where H is the subgroup of $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ corresponding to K in the Galois correspondence. In particular, $\Gamma(R,S)$ is integral if and only if $aS = S$ for each $a \in (\mathbb{Z}/n)^\times$.

Definition

A Cayley graph $\Gamma(R, S)$ is called a gcd-graph if S is stable under the action of $R^\times$.

- We can show that S is stable under the action of $R^\times$ if and only if there exists a subset $D = \{x_1, x_2, \ldots, x_k\}$ of non-associate elements in R with the property that: for each $s \in R$, $s \in S$ if and only if $sR = x_i R$ for some $x_i \in D$.
- In practice, it is often the case that S is only stable under the action of a proper subgroup U of $R^\times$. We call these graphs U-unitary Cayley graphs. In this case, the spectra of these graphs can be described by a supercharacter theory on R associated with U (joint work with Nguyen Duy Tan).

An example

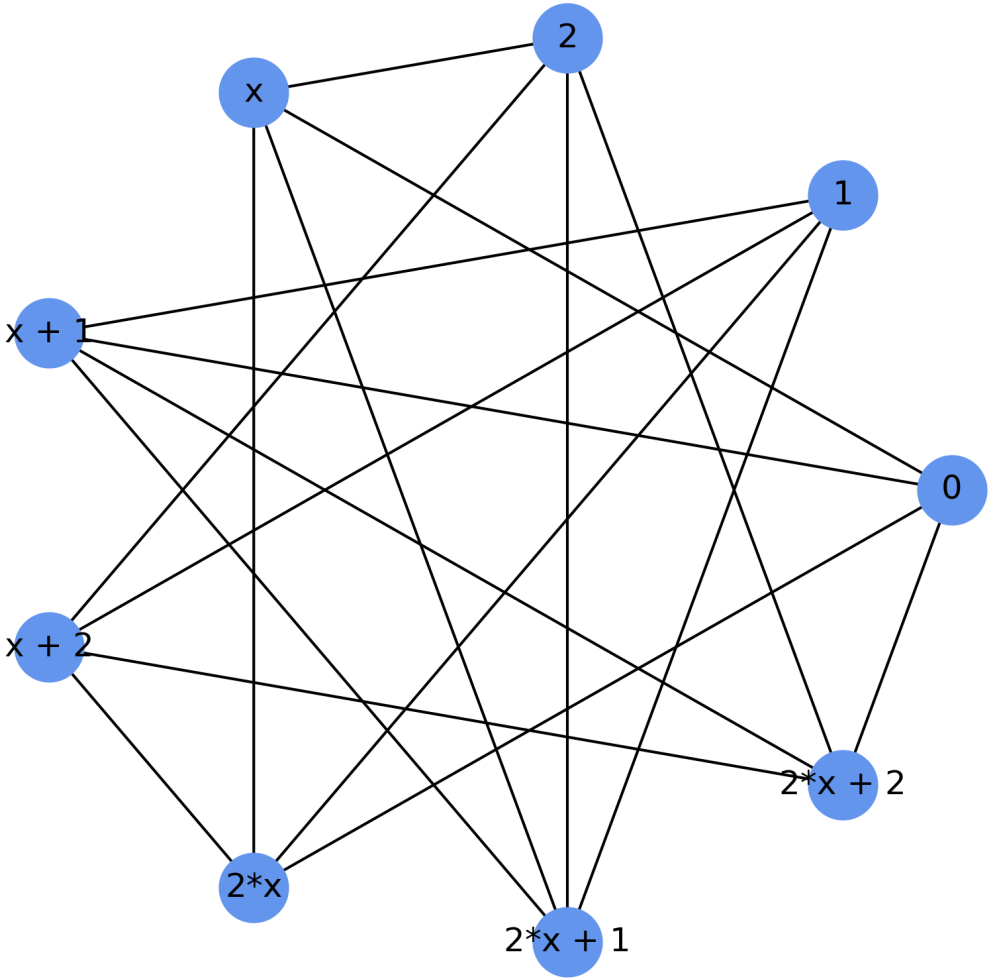

Figure 2: The gcd-graph $G_f(D)$ with $f = x(x+1) \in \mathbb{F}_3[x]$ and $D = \{x, x+1\}$

Spectra of gcd-graphs

A gcd-graph $\Gamma(R, S)$ is necessarily integral. In fact, we can say more.

Theorem (Mináč, Nguyen, Tan)

Suppose that $\Gamma(R, S)$ is a gcd-graph over R. Then, there is an explicit description of the spectrum of $\Gamma(R, S)$ via the generalized Mobius and Euler functions.

Question

Can we classify all gcd-graphs on R that have PST?

When $R = \mathbb{Z}/n$, many results are known (due to works of Godsil, Basic, Petkovic, Stevanovic, and others)

- PST can only exist between 0 and $n/2$. In particular, n must be even.
- When $S = (\mathbb{Z}/n)^{\times}$, PST exists only for $n = 2, 4$.

Theorem (Nguyen-Tan)

Let R be a finite Frobenius ring. Suppose that R has the following Artin-Wedderburn decomposition: $R = (\prod_{i=1}^{d} S_i) \times R_2$. Here, $(S_i, \mathfrak{m}_i)$ represents all local factors of R whose residue fields are $\mathbb{F}_2$. For each $1 \leq i \leq d$, let e_i be the unique minimal element of S_i.

1. *If there exists PST between 0 and some $s \in R$, then s must be of the form $(a_1, a_2, \ldots, a_d, 0)$, where each a_i is 0 or e_i. In particular, if R is a local ring, then $s = e$, where e is the unique minimal element of S.*
2. *Suppose that $(R, \mathfrak{m})$ is a principal ideal local ring with a generator α and residue field $\mathbb{F}_2$. Let n be the smallest positive integer such that $\alpha^n = 0$. Then, the gcd-graph $\Gamma(R, S)$ has PST if and only if $|S \cap \{\alpha^{n-1}, \alpha^{n-2}\}| = 1$.*

References

- Chris Godsil, State transfer on graphs. Discrete Mathematics (2012).
- Walter Klotz, Torsten Sander, Some properties of unitary Cayley graphs. The electronic journal of combinatorics (2007).
- Ján Mináč, Tung T. Nguyen, Nguyen Duy Tan, On the gcd graphs over the polynomial rings, preprint, arXiv:2409.01929
- Saxena, Nitin, Simone Severini, and Igor E. Shparlinski, Parameters of integral circulant graphs and periodic quantum dynamics. International Journal of Quantum Information (2007).
- Tung T. Nguyen, Nguyen Duy Tan, Integral Cayley graphs over a finite symmetric algebra. Arch. Math. (2025).
- Tung T. Nguyen, Nguyen Duy Tan, Gcd-graphs over finite rings, preprint, arXiv:2503.04086.
- Wasin So, Integral circulant graphs, Discrete Mathematics (2006).

Acknowledgements

We gratefully acknowledge the following organizations for their support:

- Natural Sciences and Engineering Research Council of Canada (NSERC) grant R0370A01.
- AMS-Simons Travel Grant
- Registration and travel support for this presentation was provided by the National Science Foundation.
- Vietnam National Foundation for Science and Technology Development (NAFOSTED)
- Lake Forest College for their support with an Overleaf subscription

Thank You!