On gcd-graphs over a finite ring

Tung T. Nguyen, and Nguyen Duy Tân

Elmhurst University

Discrete Math Seminar
March 2026, Iowa State University, Virtual Talk

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

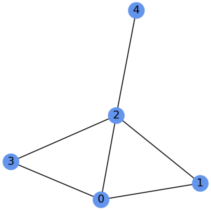

Figure 1: A random graph on $n = 5$ nodes

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

The adjacency matrix of this graph.

Graph spectra

- The spectrum of G, denoted $\mathrm{Spec}(G)$, is the set of eigenvalues of its adjacency matrix A. Equivalently, it is the set of 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 K-rational if every $\lambda \in \mathrm{Spec}(G)$ lies in $\mathcal{O}_K$, the ring of integers of K.
- A $\mathbb{Q}$-rational graph is called an integral graph.

Perfect state transfer on graphs

Definition

Let $F(t)$ be the continuous-time quantum walk associated with G; namely $F(t) = \exp(\mathrm{i}A_G t) = e^{\mathrm{i}A_G t}$. 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 $F(t) = \exp(\mathrm{i}A_G t) = \mathrm{e}^{\mathrm{i}A_G t}$. 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 $F(t) = \exp(\mathrm{i}A_G t) = e^{\mathrm{i}A_G t}$. 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.*

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

Definition

A graph G is $\mathbb{Z}/n$-circulant (in other words, a Cayley graph over $\mathbb{Z}/n$) if it is equipped with the following data:

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

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

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 $\vec{c}$.

- 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 $\mathbb{Z}/n$. We will write $G_n(D)$ for associated gcd-graph.

History of gcd-graphs

- Gcd-graphs were introduced by Klotz and Sander as a generalization of unitary Cayley graphs (corresponding to the case $D = \{1\}$). The spectrum of $G_n(D)$ is $(\lambda_m)_{m \in \mathbb{Z}/n}$ where

$$\lambda_m = \sum_{d \in D} c\left(m, \frac{n}{d}\right),$$

and

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

- This gives another direct proof that gcd-graphs are integral graphs. Furthermore, this explicit description can be used to show that the spectrum of $G_R(D)$ satisfies certain congruence properties.

An example

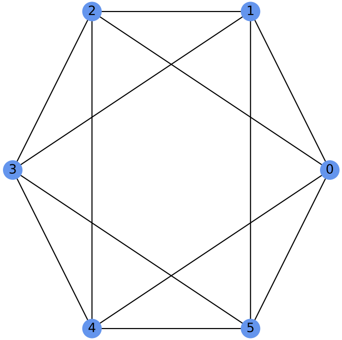

Figure 2: The gcd-graph $G_n(D)$ with $n = 6$ and $D = \{1, 2\}$

The characteristic polynomial of $G_n(D)$ is $x^3(x-4)(x+2)^2$.

Theorem (Saxena, Severini, Shparlinski)

Let $D = \{d_1, d_2, \ldots, d_r\}$ and let $G_n(D)$ be the associated gcd-graph. Then $G_n(D)$ is connected iff $\gcd(d_1, d_2, \ldots, d_r) = 1$. Furthermore, let t be the smallest integer for which there exists a subset $\{d_{i_1}, \ldots, d_{i_t}\} \subset D$ that additively generates $\mathbb{Z}/n$. Then

$$t \leq \operatorname{diam}\big(G_n(D)\big) \leq 2t + 1.$$

Gcd-graphs over a finite commutative ring

Let R be a finite commutative ring and let $S \subset R$. The Cayley graph $\Gamma(R, S)$ has vertex set R, with $u, v \in R$ adjacent if $u - v \in S$.

A natural question is: what is the "correct" definition of a gcd-graph over R? Various attempts have been made.

- Kiani, Haji Aghaei, Meemark, and Suntornpoch gave a definition when R is a quotient of a unique factorization domain D. In this case the natural definition works well; they use it to study spectra and energy.
- Suntornpoch and Meemark later gave a definition that works for finite chain rings and their direct products.
- These works rely on the fact that in those cases the gcd function is well defined.

Gcd-graphs over a finite commutative ring

Let us explain our approach. For a general commutative ring, the gcd function may not be well defined. We use ideals instead. For $a, b \in R$, say a and b have the same gcd if $Ra = Rb$. For finite rings (more generally, for Artinian rings) this is equivalent to $a = ub$ for some $u \in R^\times$. This leads to the following definition.

Definition

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

Equivalently, S is $R^\times$-stable iff there exists a set $D = \{x_1, \ldots, x_k\}$ of non-associate elements of R such that $s \in S$ iff $sR = x_i R$ for some $x_i \in D$. We write $G_R(D)$ for the resulting graph.

Some further generalizations

- If $S = R^{\times}$, the associated graph is called a unitary Cayley graph and denoted $G_R := G_R(\{1\})$. This kind of graph has been widely studied in the literature. In fact, one can trace it back to the work of Evans and Erdős, who showed that every graph is an induced subgraph of a unitary Cayley graph over $\mathbb{Z}/n$.
- In practice, it is often the case that S is stable only under the action of a proper subgroup U of $R^{\times}$. We call these graphs U-unitary Cayley graphs.
- For non-commutative rings, we will need to assume that S is stable under both the left and right actions of $R^{\times}$; namely $R^{\times} S R^{\times} = S$.

An example

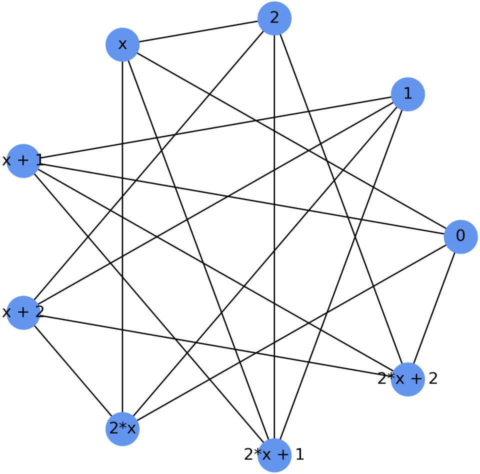

Figure 3: The gcd-graph $G_f(D)$ with $f = x(x+1) \in \mathbb{F}_3[x]$ and $D = \{x, x+1\}$

Theorem (Nguyen–Tân)

Let R be a finite commutative ring. Let $D = \{x_1, x_2, \ldots, x_r\}$ be a set of non-associate elements of R, and let S be the associated generating set. Suppose the unitary Cayley graph $G_R(\{1\})$ is connected. Then $G_R(D) := \Gamma(R, S)$ is connected if and only if the ideal generated by $x_1, x_2, \ldots, x_r$ is R.

Proof.

A Cayley graph $\Gamma(R, S)$ is connected iff the abelian group generated by S is R. Let $a \in R$. If the ideal generated by the x_i equals R, then we can write $a = \sum_{i=1}^{k} a_i x_i$ for some $a_i \in R$. Since G_R is connected, for each i we can write $a_i = \sum_{j=1}^{n_i} m_{ij} s_{ij}$ with $m_{ij} \in \mathbb{Z}$ and $s_{ij} \in R^\times$. Hence $a = \sum_{i=1}^{k} \sum_{j=1}^{n_i} m_{ij} s_{ij} x_i$, and each $s_{ij} x_i \in S$, so a lies in the subgroup generated by S. Thus $G_R(D)$ is connected. $\square$

Finite Frobenius rings

Let n be the characteristic of R and let $\zeta_n := e^{2\pi i/n}$ be a primitive nth root of unity.

Definition

A finite commutative ring R is Frobenius if there exists a $\mathbb{Z}/n$-functional $\psi : R \to \mathbb{Z}/n$ whose kernel contains no nonzero ideal of R.

- For each $r \in R$, define $\chi_r \in \widehat{R} := Hom(R, \mathbb{C}^\times)$ by

$$\chi_r(s) = \zeta_n^{\psi(rs)}.$$

- The non-degeneracy condition on $\ker(\psi)$ implies the map $R \to \widehat{R}$, $r \mapsto \chi_r$, is an isomorphism. Equivalently, R is canonically self-dual.

Finite Frobenius rings

Some examples of finite Frobenius rings.

- $R = \prod_n \mathbb{Z}/n$. Consequently, each finite abelian group is isomorphic to a $(R, +)$ where R is a finite Frobenius ring.
- R is a finite quotient of $\mathcal{O}_K$ where K is a finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$.
- If R is Frobenius and H is an abelian group then $R[H]$ is also Frobenius.
- R is semisimple, then R is Frobenius.
- Every finite commutative ring is a quotient of a finite Frobenius ring.

By the circulant diagonalization theorem, the spectrum of the Cayley graph $\Gamma(R, S)$ is the multiset $\{\lambda_r\}_{r \in R}$ where

$$\lambda_r = \sum_{s \in S} \chi_r(s) = \sum_{s \in S} \chi(rs).$$

For example, when $S = R^{\times}$ and $r = 1$, this sum equals

$$\lambda_1 = \sum_{s \in R^{\times}} \chi(s) = \sum_{s \in R^{\times}} \zeta_n^{\psi(s)}.$$

This is a Ramanujan sum (first studied by Ramanujan and later generalized by Lamprecht in his work on Gauss sums and L-functions). It turns out that $\lambda_1 = \mu(R)$, where μ is a generalization of the Möbius function.

Spectra of gcd-graphs

A gcd-graph $\Gamma(R, S)$ is necessarily integral. In fact, using Lamprecht's calculations of generalized Ramanujan sums, we can say more.

Theorem (Nguyen-Tân)

Suppose that $\Gamma(R, S)$ is a gcd-graph over R. Then

1. *There is an explicit description of the spectrum of $\Gamma(R, S)$ via the generalized Möbius and Euler functions. When $R = \mathbb{Z}/n$, this description coincides with the one obtained by Klotz and Sander.*
2. *0 is not an eigenvalue of $G_R := \Gamma(R, R^\times)$ if and only if G_R is a prime graph (namely, it has no non-trivial homogeneous sets).*

PST on gcd-graphs

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 $n = 2, 4$.

PST on gcd-graphs

- Let $G = \Gamma(R, S)$ be a Cayley graph defined over R.
- For each $r \in R$, we define

$$\vec{v}_r = \frac{1}{\sqrt{|R|}}[\zeta_n^{\psi(rs)}]_{s\in R}^T \in \mathbb{C}^{|R|}, \lambda_r = \sum_{s\in S} \zeta_n^{\psi(rs)}.$$

  Then v_r is a normalized eigenvector of A_G with λ_r being the corresponding eigenvalue.
- Let $V = [v_r]_{r\in R} \in \mathbb{C}^{|R|\times|R|}$, $D = \mathrm{diag}([\lambda_r]_{r\in R})$. Then we can write

$$A_G = VDV^* = \sum_{r\in R} \lambda_r \vec{v}_r \vec{v}_r^*,$$

- Therefore, we have

$$F(t) = \sum_{r\in R} e^{\mathrm{i}\lambda_r t} \vec{v}_r \vec{v}_r^*.$$

PST on gcd-graphs

- Let $s_1, s_2 \in R$. Then

$$F(t)_{s_1,s_2} = \frac{1}{|R|} \sum_{r \in R} e^{\mathrm{i}\lambda_r t} \zeta_n^{\psi((s_1-s_2)r)} = \frac{1}{|R|} \sum_{r \in R} e^{2\pi \mathrm{i}\left(\lambda_r \frac{t}{2\pi} + \frac{\psi((s_1-s_2)r)}{n}\right)}.$$

- By the triangle inequality, $|F(t)_{s_1,s_2}| = 1$ if and only if $\lambda_r \frac{t}{2\pi} + \frac{\psi(s_1-s_2)r}{n}$ are the same modulo 1 for all $r \in R$.
- By symmetry, there exists perfect state transfer between s_1 and s_2 if and only if there exists perfect state transfer between 0 and $s_2 - s_1$.

In summary, we have the following.

Theorem (Nguyen-Tân, Bašić-Petković-Stevanović)

Let $G = \Gamma(R, S)$ be a Cayley graph defined over a finite Frobenius ring. There exists perfect state transfer from 0 to s at time t if and only if for all $r_1, r_2 \in R$

$$(\lambda_{r_1} - \lambda_{r_2})\frac{t}{2\pi} + \frac{\psi(s(r_1 - r_2))}{n} \in \mathbb{Z}\,.$$

Corollary

Let Δ be the abelian group generated by $r_1 - r_2$ where r_1 and r_2 are elements of R such that $\lambda_{r_1} = \lambda_{r_2}$. Then $\psi(sd) = 0$ for all $d \in \Delta$. In particular, if $\Delta = R$ then there is no PST on $\Gamma(R, S)$.

PST on gcd-graphs

We recall that the spectrum of a gcd-graph $\Gamma(R, S)$ is given by $\{\lambda_r\}$ where $\lambda_r = \sum_{s \in S} \zeta_n^{\psi(rs)}$. If $t = ru$ for some $u \in R^\times$ then

$$\lambda_t = \sum_{s \in S} \zeta_n^{\psi(rus)} = \sum_{s \in uS} \zeta_n^{\psi(rs)} = \lambda_r.$$

The last equality follows from the fact that $uS = S$. This shows that Δ contains the Δ_R where Δ_R is the abelian group generated by $u_1 - u_2$ where $u_1, u_2 \in R^\times$.

Theorem (Skornyakov's question)

If R does not have $\mathbb{Z}/2$ as a quotient, then every element in R is a difference of two units. Consequently, $\Delta = \Delta_R = R$ and hence $\Gamma(R, S)$ has no PST.

Theorem (Nguyen-Tân)

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 Tân, On the gcd-graphs over the polynomial rings, The Canadian Journal of Mathematics, 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 Tân, Integral Cayley graphs over a finite symmetric algebra. Arch. Math. (2025).
- Tung T. Nguyen, Nguyen Duy Tân, Gcd-graphs over finite rings, To appear in Journal of Algebra and Its Applications, arXiv:2503.04086.
- Wasin So, Integral circulant graphs, Discrete Mathematics (2006).

Acknowledgements

We gratefully acknowledge the following organizations for their support:

- AMS-Simons Travel Grant
- Vietnam National Foundation for Science and Technology Development (NAFOSTED)

Thank You!