Spectral Graph Theory Lecture 24

Strongly Regular Graphs, part 2

Daniel A. Spielman November 20, 2009

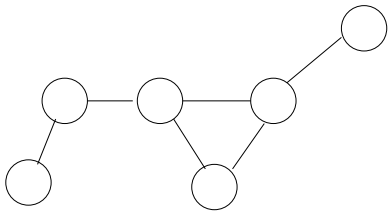
24.1 Introduction

In this lecture, I will present three results related to Strongly Regular Graphs.

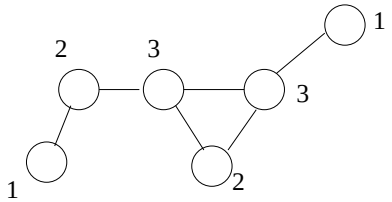
1. An algorithm for testing isomorphism of SRGs that runs in time $2^{O(\sqrt{n}\log n)}$.
2. A proof that f and g, the dimensions of the eigenspaces, are both at least $\sqrt{n}$.
3. Paley Graphs, one of the most useful families of SRGs.

24.2 Testing Isomorphism by Individualization and Refinement

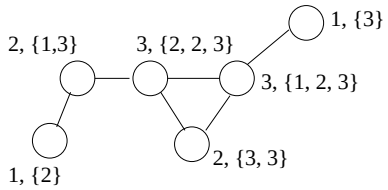
The problem of testing isomorphism of graphs is often reduced to the problem of giving each vertex in a graph a unique name. If we have a way of doing this that does not depend upon the initial ordering of the vertices, then we can use it to test graph isomorphism: find the unique names of vertices in both graphs, and then see if it provides an isomorphism. For example, consider the graph below.



We could begin by labeling every vertex by its degree.



The degrees distinguish between many nodes, but not all of them. We may refine this labeling by appending the labels of every neighbor of a node.



Now, every vertex has its own unique label. If we were given another copy of this graph, we could use these labels to determine the isomorphism between them. This procedure is called *refinement*, and it can be carried out until it stops producing new labels. However, it is clear that this procedure will fail to produce unique labels if the graph has automorphisms, or is a strongly regular graph. In these cases, we need a way to break symmetry.

The procedure called *individualization* breaks symmetry arbitrarily. It chooses some nodes in the graph, arbitrarily, to give their own unique names. Ideally, we pick one vertex to give a unique name, and then refine the resulting labeling. We could then pick another troubling vertex, and continue. We call a set of vertices $S \subset V$ a *distinguishing set* if individualizing this set of nodes results in a unique name for every vertex, after refinement. How would we use a distinguishing set to test isomorphism? Assume that S is a distinguishing set for $G = (V, E)$. To test if $H = (W, F)$ is isomorphic to G, we could enumerate over *every* possible set of $|S|$ vertices of W, and check if they are a distinguishing set for H. If G and H are isomorphic, then H will also have an isomorphic distinguishing set that can use to find an isomorphism between G and H. We would have to check $\binom{n}{|S|}$ sets, and try $|S|!$ labelings for each, so we had better hope that S is small.

24.3 Distinguishing Sets for Strongly Regular Graphs

We will now prove a result of Babai [Bab80] which says that every strongly regular graph has a distinguishing set of size $O(\sqrt{n} \log n)$. Babai's result won't require any refinement beyond naming every vertex by the set of individualized nodes that are its neighbors. So, we will prove that a set of nodes S is a distinguishing set by proving that for every pair of distinct vertices x and y, either there is an $s \in S$ that is a neighbor of x but not of y, or the other way around. This will suffice to distinguish x and y. As our algorithm will work in a brute-force fashion, enumerating over all sets of a given size, we merely need to show that such a set S exists. We will do so by proving that a random set of vertices probably works.

I first observe that it suffices to consider strongly-regular graphs with $k < n/2$, as the complement of a strongly regular graph is also a strongly regular graph (that would have been too easy to assign as a homework problem). We should also observe that every strongly-regular graph has diameter 2, and so $k \geq \sqrt{n-1}$.

Lemma 24.3.1. *Let $G = (V, E)$ be a connected strongly regular graph with n vertices and degree $k < n/2$. Then for every pair of vertices x and y, there are at least $k/6$ vertices that are neighbors of x but not y.*

Before I prove this, let me show how we may use it to prove the theorem. This lemma tells us that there are at least $\sqrt{n-1}/6$ nodes that are neighbors of x but not of y. Let T be the set of nodes

that are neighbors of X by not neighbors of Y. So, if we choose a vertex at random, the probability that it is in T is at least

$$\frac{\sqrt{n-1}}{6n} \geq \frac{1}{6\sqrt{n+2}}.$$

If we choose a set S of $6\sqrt{n+2}\ln n^2$ vertices at random, the probability that none of them is in T is

$$\left(1 - \frac{1}{6\sqrt{n+2}}\right)^{6\sqrt{n+2}\ln n^2} \leq \frac{1}{n^2}.$$

So, the probability that a random set of this many nodes fails to distinguish all pairs is at most $1/2$.

Proof of Lemma 24.3.1. If $x \sim y$, then the number of nodes that are neighbors of X but not of y is $k-1-\lambda$, and if $x \not\sim y$ the number if $k-\mu$. So, we need to prove that neither λ nor μ is too close to k.

We will do this by establishing some elementary relations between these parameters. First, consider the case in which $x \sim y$. Let z be any vertex such that $x \not\sim z$ and $y \not\sim z$. We will use z to prove an upper bound on the number of vertices w that are neighbors of x but not of y. Let

$$Z_0 = \{w : w \sim x, w \not\sim z\}, \quad \text{and} \quad Z_1 = \{w : w \not\sim y, w \sim z\}.$$

Clearly, every w that is a neighbor of x but not of y lies in either Z_0 or Z_1. As z is neither a neighbor of x nor of y,

$$|Z_0| = |Z_1| = k - \mu.$$

So,

$$k - \lambda - 1 \leq 2(k-\mu) \quad \Longrightarrow \quad 2\mu \leq k + \lambda + 1. \tag{24.1}$$

So, if μ is close to k, λ must also be close to k.

We can similarly obtain an inequality in the other direction when $x \not\sim y$ by exploiting a z such that $z \sim x$ and $z \sim y$. Now, for any $w \sim x$ but $w \not\sim y$, we have either

$$(w \sim x \text{ and } w \not\sim z) \text{ or } (w \sim z \text{ and } w \not\sim y).$$

So,

$$k - \mu \leq 2(k - \lambda - 1) \quad \Longrightarrow \quad 2(\lambda + 1) \leq k + \mu. \tag{24.2}$$

This tells us that if λ is close to k, then μ is also.

We require one more relation between λ and μ. We obtain this relation by picking any vertex x, and counting the pairs y, z such that $y \sim z$, $x \sim y$ and $x \not\sim z$. Every node y that is a neighbor of x has λ neighbors in common with x, and so has $k - \lambda - 1$ neighbors that are not neighbors of x. This gives

$$|\{(y,z) : y \sim z, x \sim y, x \not\sim z\}| = k(k - \lambda - 1).$$

On the other hand, there are $n - k - 1$ nodes z that are not neighbors of x, and each of them has μ neighbors in common with x, giving

$$|\{(y,z) : y \sim z, x \sim y, x \not\sim z\}| = (n - k - 1)\mu.$$

Combining, we find

$$(n-k-1)\mu = k(k-\lambda-1). \tag{24.3}$$

As $k < n/2$, this equation tells us

$$k(k-\lambda-1) \geq k\mu \quad \Longrightarrow \quad k-\lambda-1 \geq \mu.$$

By adding this to inequality 24.1, we obtain

$$2k \geq 3\mu \quad \Longrightarrow \mu \leq \frac{2}{3}k.$$

By now applying inequality 24.2, we may prove

$$\lambda + 1 \leq \frac{5}{6}k.$$

□

Note that the constants in this bound can be tightened. In particular, one may prove $\lambda \leq 2k/3$.

I [Spi96] improved this bound to $n^{1/3}\log n$ by exploiting one more round of refinement, and proving additional inequalities the parameters must satisfy. These inequalities hold for all but some special families of SRGs, such as Latin Square Graphs, but these can be treated separately.

24.4 Two-distance point sets

Recall from last lecture that each eigenspace of a strongly regular graph supply a set of points on the unit sphere such that the distance between a pair of points just depends on whether or not they are adjacent. If the graph is connected and not the complete graph, then we can show that these distances are greater than zero, so no two vertices map to the same unit vector. If we take the corresponding point sets for two strongly regular graphs with the same parameters, we can show that the graphs are isomorphic if and only if there is an orthogonal transformation that maps one point set to the other. In low dimensions, it is easy to find such an orthogonal transformation if one exists.

Consider the eigenspace of r, which we recall has dimension f. Fix any set of f independent vectors corresponding to f vertices. An orthogonal transformation is determined by its action on these vectors. So, if there is an orthogonal transformation that maps one vector set onto the other, we will find it by examining all orthogonal transformations determined by mapping these f vectors to f vectors in the other set. Thus, we need only examine $\binom{n}{f} f!$ transformations. This would be helpful if f were small. Unfortunately, it is not. We will now prove that both f and g must be at least $\sqrt{2n} - 2$.

Let $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^n$ be a set of unit vectors in $\mathbb{R}^f$ such that there are two values $\alpha, \beta < 1$ such that

$$\left\langle \boldsymbol{x}^i, \boldsymbol{x}^j \right\rangle = \ \alpha \ \text{ or } \ \beta.$$

We will prove a lower bound on f in terms of n.

The key to our proof is to define an f-variate polynomial for each point. In particular, we set

$$p_i(\boldsymbol{y}) = (\boldsymbol{y}^T \boldsymbol{x}^i - \alpha)(\boldsymbol{y}^T \boldsymbol{x}^i - \beta),$$

for $\boldsymbol{y} \in \mathbb{R}^f$. We first note that each polynomial p_i is a polynomial of degree 2 in f variables (the coordinates of $\boldsymbol{y}$). As each f-variate polynomial of degree 2 can be expressed in the form

$$a + \sum_i b_i y_i + \sum_{i \leq k} c_{i,j} y_i y_j,$$

we see that the vector space of degree-2 polynomials in f variables has dimension

$$1 + 2f + \binom{f}{2}.$$

To prove a lower bound on f, we will show that these polynomials are linearly independent. Assume by way of contradiction that they are not. Then, without loss of generality, there exist coefficients $\gamma_1, \ldots, \gamma_n$ with $\gamma_1 \neq 0$ and

$$\sum_i \gamma_i p_i(y) = 0.$$

To obtain a contradiction, plug in $y = \boldsymbol{x}^1$, to find

$$\sum_i \gamma_i p_i(\boldsymbol{x}^1) = \gamma_1 p_1(\boldsymbol{x}^1) \neq 0.$$

Thus, we may conclude

$$n \leq 1 + 2f + \binom{f}{2},$$

which implies

$$f \geq \sqrt{2n} - 2.$$

24.5 Paley Graphs

Paley graphs are Cayley graphs of $\mathbf{Z}/p$, the numbers modulo a prime, for a prime p that is equivalent to 1 modulo 4. They are generated by the set of squares modulo p,

$$S = \left\{x^2 : x \in \mathbf{Z}/p\right\}.$$

That is, $V = \mathbf{Z}/p$ and (u, v) is an edge if $u - v$ is the square of some number modulo p. I will explain why this graph is a Strongly Regular Graph. But first, I should just explain why it is a graph.

To do this, I need to tell you a little about $\mathbf{Z}/p$. Here is the key fact that we need.

Fact 24.5.1. *For every prime p, there exists a number g such that for every number x between 1 and $p-1$, there is an i between 1 and $p-1$ such that*

$$x \equiv g^i \mod p.$$

In particular, $g^{p-1} \equiv 1$.

Corollary 24.5.2. *If p is a prime equivalent to 1 modulo 4, then -1 is a square modulo p.*

Proof. We know that 4 divides $p-1$. Let $s = g^{(p-1)/4}$. I claim that $s^2 = -1$. This will follow from $s^4 = 1$.

To see this, consider the equation

$$x^2 - 1 \equiv 0 \mod p.$$

As the numbers modulo p are a field, it can have at most 2 solutions. Moreover, we already know two solutions, $x = 1$ and $x = -1$. As $s^2 = 1$, we know that s^2 must be one of 1 or -1. However, it cannot be the case that $s^2 = 1$, because then the powers of g would begin repeating after the $(p-1)/2$ power, and thus could not represent every number modulo p. □

We now understand a lot about the squares modulo p (formally called *quadratic residues*). The squares are exactly the elements g^i where i is even. As $g^i g^j = g^{i+j}$, the fact that -1 is a square implies that x is a square if and only if $-x$ is a square. So, S is closed under negation, and the Cayley graph of $\mathbf{Z}/p$ with generator set S is in fact a graph. As $|S| = (p-1)/2$, it is regular of degree

$$k = \frac{p-1}{2}.$$

We now move to proving that it is strongly regular. Consider two vertices, say x and y. Instead of directly computing for how many elements z both $x - z$ and $y - z$ are squares, we will compute the number of elements z such that $(x-z)(y-z)$ is a square. As we know the degree of x and y, this will enable us to determine the number of common neighbors of x and y. To see this, let X be the neighbors of x, Y be the set of neighbors of y, and let Z be the set of nodes $(X \cap Y) \cup (\bar{X} \cap \bar{Y})$. We have

$$\begin{aligned}
|Z| &= \left|(X \cap Y) \cup (\bar{X} \cap \bar{Y})\right| \\
&= |X \cap Y| + \left|(\bar{X} \cap \bar{Y})\right| \\
&= |X \cap Y| + p - |X \cup Y| \\
&= |X \cap Y| + p - |X| - |Y| + |X \cap Y| \\
&= 2\,|X \cap Y| + p - 2(p-1)/2 \\
&= 2\,|X \cap Y| + 1.
\end{aligned}$$

We will now prove that

$$|Z| = \begin{cases} k-1 & \text{if } x-y \text{ is a square} \\ k & \text{if } x-y \text{ is not a square.} \end{cases}$$

To do this, we define the function

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \text{ is a square modulo } p \\ -1 & \text{otherwise.} \end{cases}$$

We first consider the case in which $x \sim y$. In this case, x and y are not in Z. So,

$$|Z| = \sum_{z \notin \{x,y\}} \frac{1}{2}\left(1 + f((x-z)(y-z))\right) = \frac{p-2}{2} + \frac{1}{2}\left(\sum_{z} f((x-z)(y-z))\right).$$

For $z \neq y$, $f(y-z) = f(1/(y-z))$, so

$$\sum_{z \notin \{x,y\}} f((x-z)(y-z)) = \sum_{z \notin \{x,y\}} f\left(\frac{x-z}{y-z}\right) = \sum_{z \notin \{x,y\}} f\left(1 + \frac{x-y}{y-z}\right).$$

By making the change of variables

$$z = y - \frac{x-y}{w-1},$$

you can verify that as z ranges over the elements different from x and y, $1 + \frac{x-y}{y-z}$ ranges over all elements different from 0 and 1. So, this last sum is

$$\sum_{w \notin \{0,1\}} f(w) = -1,$$

as exactly half of the non-zero elements are squares, and we have omitted 1 from the sum. This gives us

$$|Z| = \frac{p-2}{2} - \frac{1}{2} = \frac{p-3}{2} = k - 1.$$

So,

$$\lambda = |X \cap Y| = \frac{k}{2} - 1.$$

On the other hand, when $x \not\sim y$, $\{x, y\} \in Z$

$$|Z| = 2 + \sum_{z \notin \{x,y\}} \frac{1}{2}\left(1 + f((x-z)(y-z))\right),$$

and we get

$$\mu = \frac{k}{2}.$$

So, these graphs are strongly regular. From μ and λ, we can compute that these graphs have eigenvalues

$$-\frac{1}{2} \pm \frac{\sqrt{2k+1}}{2} = -\frac{1}{2} \pm \frac{\sqrt{p}}{2}.$$

These eigenvalues values are almost as small as possible, and have been used by Chung, Graham and Wilson [CGW89] to show that these graphs have many pseudo-random properties.

References

[Bab80] László Babai. On the complexity of canonical labeling of strongly regular graphs. *SIAM Journal on Computing*, 9(1):212–216, 1980.

[CGW89] F. R. K. Chung, R. L. Graham, and R. M. Wilson. Quasi-random graphs. *Combinatorica*, 9(4):345–362, 1989.

[Spi96] Daniel A. Spielman. Faster isomorphism testing of strongly regular graphs. In *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 576–584, New York, NY, USA, 1996. ACM.