REU 2006 · Discrete Math · Lecture 7

Instructor: László Babai
Scribe: Elizabeth Beazley
Editors: Sourav Chakraborty and Elizabeth Beazley
NOT PROOF-READ

July 11, 2006. Last updated July 10, 2006 at 1:00 p.m.

7.1 Results on Polynomials

Claim 7.1.1. *Let* $f(x) = x^4 + ax^3 + bx^2 + cx - 15$ *where* $a, b, c \in \mathbb{Z}$. *If* $f(t) = 0$ *for some* $t \in \mathbb{Q}$ *then*

1. $t \in \mathbb{Z}$, *and*

2. $t|15$.

Proof. Since t is rational we can write t as $\frac{r}{s}$, where $r, s \in \mathbb{Z}$ and $\gcd(r, s) = 1$. If we plug this into the equation $f(t) = 0$, we get

$$r^4 + ar^3s + br^2s^2 + crs^3 - 15s^4 = 0$$

$$\implies r^4 = -s(ar^3 + br^2s + crs^2 - 15s^3) \tag{7.1.1}$$

Thus, $s|r^4$, but since $\gcd(r, s) = 1$, it follows that $s = \pm 1$. We can assume WLOG that $s > 0$ so that $t = r \in \mathbb{Z}$. This proves part (1) of the claim.

For proving part (2) we consider the equation $f(r) = r^4 + ar^3 + br^2 + cr - 15 = 0$. By rearranging we get

$$15 = r(r^3 + ar^2 + br + c)$$

Since $r \in \mathbb{Z}$ we get from the above equation $r|15$, and in particular, $r \in \{\pm 1, \pm 3, \pm 5, \pm 15\}$. □

Corollary 7.1.2. If $u \in \mathbb{Q}$ and $u^2 \in \mathbb{Z}$, then $u \in \mathbb{Z}$.

Proof. u is a rational root of the polynomial $f(x) = x^2 - u^2$. So if we apply the previous claim to this polynomial we get $u \in \mathbb{Z}$. □

7.2 Hoffman-Singleton Theorem

Definition 7.2.1. The **girth** of a graph is the minimum size cycle that exist in the graph.
For example a graph with girth (≥ 5) means that there is no cycle of length 3 or 4.
The girth of a tree is ∞.

Definition 7.2.2. A graph is called r**-regular** if every vertex has degree r.

Question 7.2.3. Let G be an r-regular graph on n vertices with girth ≥ 5. What graphs G also satisfy that $n = r^2 + 1$?

For the cases $r = 1$, $r = 2$, and $r = 3$, the graphs are the single edge graph on two vertices, the pentagon and the Peterson's Graph respectively. (Figure 1).

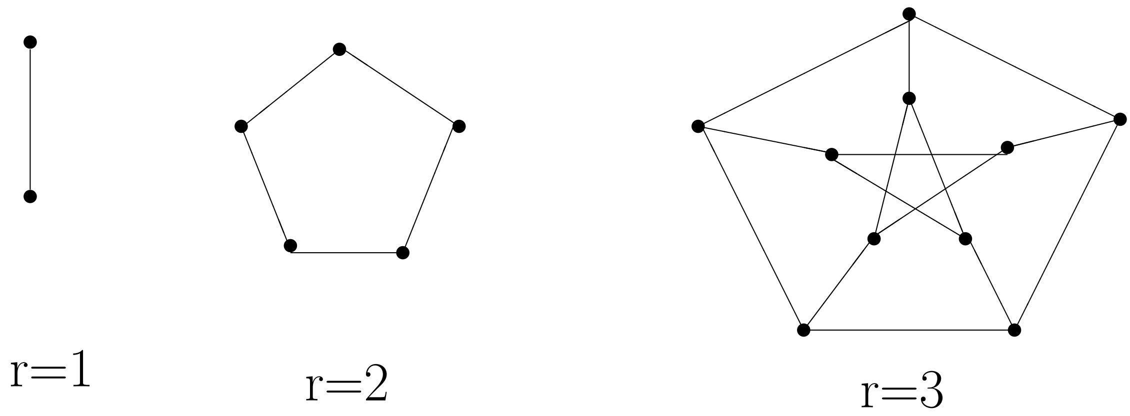

Figure 1: Graphs for r=1, 2, 3

No such graphs exist for $r = 4, 5, 6$. For $r = 7$, the resulting graph is called the *Hoffman-Singleton graph.*
The following theorem answers the Question 7.2.3

Theorem 7.2.4 (Hoffman-Singleton). *Let G be a r-regular graph on n vertices with girth ≥ 5. If $n = r^2 + 1$, then $r \in \{1, 2, 3, 7, 57\}$.*

7.3 Review of Linear Algebra

Let A be an $n \times n$ real matrix.

Definition 7.3.1. $\lambda \in \mathbb{R}$ is an **eigenvalue** and $\underline{x} \in \mathbb{R}^n$ is a corresponding **eigenvector** of the matrix A if $\underline{x} \neq 0$ and $A\underline{x} = \lambda\underline{x}$.

We can think about A as a map $A : \mathbb{R}^n \longrightarrow \mathbb{R}^n$. To say that $\underline{x}$ is an eigenvector of A means that $A\underline{x} - \lambda I\underline{x} = 0$, where I is the identity matrix. Equivalently, $(A - \lambda I)\underline{x} = 0$, or $(\lambda I - A)\underline{x} = 0$.

In general, consider a matrix $B = (\underline{b}_1 \cdots \underline{b}_n)$, where the $\underline{b}_i \in \mathbb{R}^n$ are column vectors. Then write $B\underline{x} = \sum \underline{b}_i x_i$. We can then see that $(\exists \underline{x} \neq 0)(B\underline{x} = 0) \iff$ the columns of B are linearly dependent. Equivalently, $(\exists \underline{x} \neq 0)(B\underline{x} = 0) \iff \det(B) = 0$. Applying this observation to our matrix equation $(\lambda I - A)\underline{x} = 0$, we see that $(\exists \underline{x} \neq 0)(\lambda I - A)\underline{x} = 0 \iff \det(\lambda I - A) = 0$.

Let us write this out explicitly for the 2×2 case. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ Then $\det(\lambda I - A) = \det \begin{pmatrix} \lambda - a & -b \\ -c & \lambda - d \end{pmatrix} = (\lambda - a)(\lambda - d) - bc = \lambda^2 - (a + d)\lambda + (ad - bc)$. For the $n \times n$ case we introduce the following defintion.

Definition 7.3.2. Let A be an $n \times n$ matrix. Then we define $f_A(t) := \det(tI - A)$ as the **characteristic polynomial of A**.

Note that the characteristic polynomial has degree n.

Theorem 7.3.3. *λ is an eigenvalue of $A \iff f_A(\lambda) = 0$.*

Let's consider this polynomial over $\mathbb{C}$. The polynomial will factor into a product of n linear factors:

$$f_A(t) = (t - \lambda_1)(t - \lambda_2) \cdots (t - \lambda_n)$$

The eigenvalues λ_i have **multiplicity** according to how many times they occur as a root of the characteristic polynomial.

Now write $A = (a_{ij})$. Let us consider

$$\det(tI - A) = \det \begin{pmatrix} t - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & t - a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \dots & t - a_{nn} \end{pmatrix} = t^n - \sum a_{ii} t^{n-1} + \cdots . \qquad (7.3.1)$$

Examine the second coefficient in the characteristic polynomial. We define the **trace** of a matrix $A = (a_{ij})$, denoted $\mathrm{Tr}(A)$, to be the sum of the diagonal entries. That is, $\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{ii}$. In light of Theorem 7.3.3, we have the following:

Corollary 7.3.4. $\mathrm{Tr}(A) = \sum_{i=1}^{n} \lambda_i$.

Exercise 7.3.5. $\prod_{i=1}^{n} \lambda_i = \det A$

Definition 7.3.6. We say that an $n \times n$ real matrix $A = (a_{ij})$ is **symmetric** if $a_{ij} = a_{ji}$. Equivalently, a symmetric matrix satisfies $A = A^t$, where A^t denotes the **transpose** of the matrix, or the reflection across the main diagonal, which interchanges rows and columns.

Definition 7.3.7. The **standard inner product** on $\mathbb{R}^n$ is defined to be $\underline{x} \cdot \underline{y} := \sum_{i=1}^{n} x_i y_i = \underline{x}^t \underline{y}$.

This inner product satisfies left distributivity; *i.e.*, $\underline{x} \cdot (\underline{y} + \underline{z}) = \underline{x} \cdot \underline{y} + \underline{x} \cdot \underline{z}$.

Definition 7.3.8. We say that two vectors $\underline{x}$ and $\underline{y}$ are **orthogonal** if $\underline{x} \cdot \underline{y} = 0$, and we write $x \perp y$.

Definition 7.3.9. We define the **Euclidean norm** on a vector $\underline{x} \in \mathbb{R}^n$ to be $||x|| := \sqrt{\underline{x} \cdot \underline{x}} = \sqrt{\sum_{i=1}^{n} x_i^2}$.

Definition 7.3.10. The vectors $\underline{e_1}, \ldots, \underline{e_k}$ are **orthonormal** if

$$\underline{e_i} \cdot \underline{e_j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

That is, $||e_i|| = 1$ and $e_i \perp e_j$ if $i \neq j$.

Definition 7.3.11. We say that we have a **basis** for $\mathbb{R}^n$ if we have n vectors in $\mathbb{R}^n$ that are linearly independent. An **eigenbasis** is a basis that consists of eigenvectors.

Theorem 7.3.12 (Spectral Theorem). *If A is a real symmetric matrix, then A has an orthonormal eigenbasis.*

Exercise 7.3.13. Prove that the matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ has no eigenbasis. In general, the matrix consisting of only 1's above the diagonal and 0's elsewhere has no eigenbasis.

7.4 Connection between graph theory and linear algebra

Definition 7.4.1. The **adjacency matrix** of a graph G is defined to be $A_G = (a_{ij})$, where

$$a_{ij} = \begin{cases} 1 & \text{if } i \sim j \\ 0 & \text{otherwise} \end{cases}$$

Here, $i \sim j$, if the vertices i and j are adjacent.

Let A_G be the adjacency matrix of the graph G. Let us consider $A_G^2 = B = (b_{ij})$, where $b_{ij} = \sum_{i=1}^{n} a_{ik} a_{kj}$. So,

$$b_{ii} = \sum a_{ik}^2 = \sum_{k=1}^{n} a_{ik} = \deg(i) \tag{7.4.1}$$

And in particular, note that

$$b_{ij} = \text{number of common neighbors of } i \text{ and } j \tag{7.4.2}$$

Theorem 7.4.2. *If G is a r-regular graph, or equivalently if the sum of each row is in A_G is r, then* $A_G \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} r \\ r \\ \vdots \\ r \end{pmatrix} = r\underline{1}$, *where* $\underline{1} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$. *Thus $\underline{1}$ is an eigenvector with eigenvalue r.*

Exercise 7.4.3. Suppose that G is regular of degree r.

(1) Then the eigenvalue r is **simple**, or has multiplicity 1, if and only if G is connected.
(2) All eigenvalues λ_i satisfy $|\lambda_i| \leq r$.
(3) Then $-r$ is an eigenvalue in the case of a connected graph $G \iff G$ is bipartite.

7.5 Proof of Hoffman-Singleton Theorem 7.2.4

Let G be a r-regular graph on n vertices with no cycles of size 3 or 4. Let $n = r^2 + 1$.

Observation 7.5.1. Note that since $n = r^2 + 1$ and the graph has no 3 and 4 cycles, if i and j are two adjacent vertices in G then they have no common neighbor. And if i and j are not adjacent, then they have a unique common neighbour.

Let A be the adjacency matrix of the graph G. Now suppose $A^2 = B = (b_{ij})$. Now from Equation 7.4.1 and 7.4.2 and Observation 7.5.1 we have $b_{ii} = r$ and

$$b_{ij} = \text{number of common neighbours of } i \text{ and } j = \begin{cases} 0 & \text{if } i \sim j \\ 1 & \text{if } i \not\sim j \text{ and } i \neq j \end{cases}$$

Denote by J the $n \times n$ matrix that has all entries 1. Then $A^2 = J - A + (r-1)I$ is satisfied by the adjacency matrix. Rewriting this matrix equation yields

$$A^2 + A - (r-1)I = J \tag{7.5.1}$$

Suppose that $A\underline{x} = \lambda\underline{x}$. Then $A^2\underline{x} = A(A\underline{x}) = A(\lambda\underline{x}) = \lambda(A\underline{x}) = \lambda(\lambda\underline{x}) = \lambda^2\underline{x}$. Thus we have that $A\underline{1} = r \cdot \underline{1}$, and $A^2\underline{1} = r^2\underline{1}$. Then from the above equation and Theorem 7.4.2 we get,

$$\begin{array}{rrcl} & A^2 \cdot \underline{1} & = & J \cdot \underline{1} - A \cdot \underline{1} + (r-1)I \cdot \underline{1} \\ \iff & r^2\underline{1} & = & n\underline{1} - r\underline{1} + (r-1)\underline{1} \\ \iff & r^2\underline{1} & = & (n-1)\underline{1} \\ \iff & r^2 & = & n-1 \end{array}$$

which we already knew.

Now let the eigenvectors of A be $\underline{1} = e_0, e_1, \ldots, e_{r^2}$, and the corresponding eigenvalues be $r = \lambda_0, \ldots, \lambda_{r^2}$. By the Spectral Theorem we know that $e_i \perp \underline{1}$ for $i \neq 0$. Thus, for $i \neq 0$,

$$Je_i = 0$$

So that the matrix equation 7.5.1 yields:

$$A^2 e_i = \lambda_i^2 e_i = 0 - \lambda_i e_i + (r-1)e_i = \lambda_i + (r-1)e_i \tag{7.5.2}$$

Solving the equation we get $\lambda_i^2 = -\lambda_i + (r-1) \iff \lambda_i^2 + \lambda_i - (r-1) = 0$. So the eigenvalues λ_i are roots of the equation $t^2 + t - (r-1) = 0$. Thus if we solve for t, we get that $t_{1,2} = \frac{-1 \pm \sqrt{1+4(r-1)}}{2} = \frac{-1 \pm \sqrt{4r-3}}{2}$ and consequently $\lambda_i \in \{t_1, t_2\}$. Thus there are only three eigenvalues. The eigenvalue r has multiplicity 1 by Exercise 7.4.3. Now suppose that m_i are the multiplicities of the eigenvalues t_i for $i = 1, 2$. Then $n = \#$ eigenvalues and in particular,

$$n = m_1 + m_2 + 1 \tag{7.5.3}$$

Note that $\mathrm{Tr}(A) = 0$ (since all diagonal entries are 0, because no vertices are adjacent to themselves). Also, by Corollary 7.3.4, we have that

$$r + m_1 t_1 + m_2 t_2 = \mathrm{Tr}(A) = 0 \tag{7.5.4}$$

Now we solve the equations 7.5.3 and 7.5.4. We write $r^2 = m_1 + m_2$ from Equation 7.5.3. Also let $\frac{-1 \pm \sqrt{4r-3}}{2} = \frac{-1 \pm s}{2}$, where $s = \sqrt{4r-3}$, or equivalently that $r = \frac{s^2+3}{4}$. Then we can substitute into the above equations to obtain:

$$\begin{array}{rrcl} & r + \frac{m_i}{2}(-1+s) + \frac{m_2}{2}(-1-s) & = & 0 \\ \iff & r - \frac{m_1+m_2}{2} + \frac{m_1-m_2}{2}s & = & 0 \\ \iff & r - \frac{r^2}{2} + \frac{m_1-m_2}{2}s & = & 0 \\ \iff & 2r - r^2 + (m_1-m_2)s & = & 0 \end{array}$$

We can solve this last equation explicitly for s unless $m_1 = m_2$. Hence we have two cases:

Case 1: If $m_1 = m_2$, then we get $2r - r^2 = 0 \iff r^2 = 2r \iff r = 0$ or 2, and so $r = 2$. This is the case of the pentagon, which we have already seen.

Case 2: If $m_1 \neq m_2$, then write $r = \frac{s^2+3}{4}$, and inserting this into the above equation yields:

$$\begin{array}{rrcl} & 2(\frac{s^2+3}{4}) - (\frac{s^2+3}{4})^2 + (m_1-m_2)s & = & 0 \\ \implies & 8s^2 + 24 - s^4 - 6s^2 - 9 + 16(m_1-m_2)s & = & 0 \\ \implies & s^4 - 2s^2 - 16(m_1-m_2)s - 15 & = & 0 \end{array}$$

Now if $s \geq 0$, then we know from Claim 7.1.1 that $s|15$. Thus, our possible choices for pairs (s, r) in this case are $(1,1), (3,3), (5,7)$, and $(15,57)$. Together with the choice $r = 2$ from Case 1, we have obtained the complete list of possible values for r in the Hoffman-Singleton Theorem.