L-OH02

Contents

We work over the complex numbers. An algebraic number is a zero of polynomial with integer coefficients. An algebraic integer is a zero of a monic polynomial with integer coefficients. Thus an algebraic integer is an algebraic number.

examples: $\sqrt{2}$, $\frac{1+\sqrt{5}}{2}$

We relate eigenvalue of polynomials to eigenvalues of matrices. If $p(t)$ is a monic polynomial, say

$$p(t) = t^d + p_1 t^{d-1} + \dots + p_d$$

then its companion matrix is

$$C_p := \begin{bmatrix} 0 & 0 & \cdots & 0 & -p_d \\ 1 & 0 & \cdots & 0 & \vdots \\ 0 & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -p_1 \end{bmatrix}$$

det

$$\left[\begin{array}{c|c} 0 \cdots 0 & -p_d \\ \hline I_{d-1} & \begin{matrix} \vdots \\ -p_1 \end{matrix} \end{array}\right]$$

trace

Lemma If p is a polynomial, then $\phi(C_p, t) = p(t)$.

All eigenvalues of C_p have geometric multiplicity one.

(So $p(t)$ is the minimal polynomial of C_p.) $\square$

Corollary A complex number is an algebraic integer if & only if it is a zero of an integer matrix. It is an algebraic number if it is a zero of a rational matrix. $\square$

Corollary If β is an algebraic number, there is an integer m such that $m\beta$ is an algebraic integer. $\square$

Since the eigenvalues of $A\otimes I - I\otimes B$ are the differences $\lambda-\mu$, where λ is an eigenvalue of A and μ an eigenvalue of B, and since the eigenvalues of $A\otimes B$ are products..., we have:

Theorem The algebraic integers form a ring; the algebraic numbers form a field.

Proof. For the second claim, the inverse of an invertible rational matrix is rational. $\square$

Remark The algebraic number are the field of fractions of the ring of algebraic integers.

Theorem If the entries of the square matrix A are algebraic integers, its eigenvalues are algebraic integers. $\square$

normal closure

Suppose α is an algebraic integer (satisfying a monic integer polynomial of degree d, say). If f & g are monic polynomials with $f(\alpha) = g(\alpha) = 0$ and $h = \gcd(f, g)$, then h is monic & $h(\alpha) = 0$. So there is a unique monic polynomial h of least degree such that $h(\alpha) = 0$. We call it the minimal polynomial of α. It is irreducible over $\mathbb{Q}$. (why?)

Lemma If an algebraic integer is rational, it is an integer.

$$\tau^3 + a\tau^2 + b\tau + c = 0$$

$$\tau = x/y \ ; \ x, y \in \mathbb{Z}, \ (x, y) = 1$$

$$x^3 + ax^2y + bxy^2 + cy^3 = 0$$

Lemma Suppose α is an algebraic integer with minimal polynomial $\psi(t)$. If α is an eigenvalue of an integer matrix A, then $\psi(t) \mid \phi(A,t)$. $\square$

So $2^{1/3}$ is not an eigenvalue of a graph.

Two algebraic integers are conjugate if they have the same minimal polynomial, and this happens if & only if there is a field automorphism that sends one to the other.

Periodicity and integrality

A subset state is a density that is diagonal and has exactly c entries equal to $1/c$, all other entries zero. So if D is a subset state, there is a subset S of $V(X)$ such that $(D)_{a,a} = \frac{1}{|S|}$ if $a \in S$ and all other vertices are zero. We will denote such a state by D_S, and may abuse notation and use to refer to the matrix $\sum_{a \in S} e_a e_a^T$ (which is psd, with trace $|S|$).

Vertex states are the simplest examples of subset states. Substate are real and hence if we have perfect state transfer between subset states at time τ, both state are periodic at time 2τ. Further both states have the same eigenvalue support.

A quadratic integer is a zero of a monic polynomial of degree two over $\mathbb{Z}$. (So it's an algebraic integer)

$\circledast$ We assume now that our Hamiltonian has entries non-negative integers.

Theorem Let D_ρ be a periodic subset state and let $\mathcal{L}$ be its eigenvalue support. Then the eigenvalues involved in $\mathcal{L}$ are either:

(θ_r, θ_s)

$E_r^\alpha D E_s^\alpha \neq 0$

(a) all integers, or

(b) there is a positive square-free integer Δ, an integer a, and integers $b_0, \ldots, b_d$, such that each eigenvalue in the eigenvalue support has the form $\frac{a + b_r\sqrt{\Delta}}{2}$.

Proof Assume the ratio condition holds.

(a) If eigenvalues θ_k & θ_ℓ are integers, then

$E_r D \neq 0 \Rightarrow \theta_r$ is e'val supp

$$\frac{\theta_r - \theta_s}{\theta_k - \theta_l} \in \mathbb{Q}$$

implies $\theta_r - \theta_s \in \mathbb{Q}$ for all r & s. So all eigenvalues are integers Why?

(b) Assume at most one eigenvalue is an integer.

We show that $(\theta_0 - \theta_1)^2$ is an integer.

For each pair of eigenvalues θ_r & θ_s, there is a non-zero rational number $a_{r,s}$ such that

$$\theta_r - \theta_s = a_{r,s}(\theta_1 - \theta_0)$$

and so

$$\prod_{r \neq s} (\theta_r - \theta_s) = (\theta_1 - \theta_0)^{d^2-d} \prod a_{r,s}$$

The product on the left is fixed by any field automorphism, and is therefore an integer. Therefore $(\theta_1 - \theta_0)^{d^2-d} \in \mathbb{Q}$.

Since $(\theta_1-\theta_0)^{d^2-d}$ is an algebraic integer, it follows that $(\theta_1-\theta_0)^{d^2-d}$ is an integer.

Assume m is the least positive integer such that $(\theta_1-\theta_0)^m \in \mathbb{Z}$. Then there are m distinct conjugates of $\theta_0-\theta_1$ of the form $\beta e^{2\pi i k/m}$ $(k=0,\dots,m-1)$, where β is the real m-th root of an integer. Since the elements of $\mathcal{L}$ are real and closed under conjugates, $m \leq 2$.

(c) Since

$$(\theta_r - \theta_s)^2 = a_{r,s}^2 (\theta_1 - \theta_0)^2$$

we see that $(\theta_r - \theta_s)^2$ is rational, and is therefore an integer. It has the same square-free part as $(\theta_1 - \theta_0)^2$, and consequently there is a square-free integer Δ (could be 1) such that for each r,

$$\theta_r - \theta_0 = m_r \sqrt{\Delta} \qquad (m_r \in \mathbb{Z})$$

Then

$$\theta_r = \theta_0 + m_r\sqrt{\Delta}$$

Assume there are exactly m eigenvalues in $\mathcal{L}$.

Summing this equation over θ_r yields

$\{\theta_r : E_r D \neq 0\}$

$$\sum_r{}' \theta_r = m\theta_0 + \sqrt{\Delta}\sum{}' m_r.$$

As $\sum' \theta_r \in \mathbb{Z}$, we see that $\theta_0 \in \mathbb{Q}(\sqrt{\Delta})$, & hence

$\theta_r \in \mathbb{Q}(\sqrt{\Delta})$ for all r. $\square$

Finiteness

Corollary Fix integers k & s. There are only finitely many connected graphs with maximum valency k & with a periodic subset state of size s.

Proof Let S be a periodic subset state of size s and let r be the covering radius of S. Let D be diagonal 01 with $D_{aa} = 1$ if & only if $a \in S$.

(a) The matrices $D, \ldots, A^r D$ are linearly independent and lie in the span of $\{E_r D : E_r D \neq 0\}$

$(E_s D)^T$

$E_r D E_s = E_r D \cdot D E_s$

If $E_r D E_s \neq 0$, then $E_r D \neq 0$ $(D^2 = D)$ and therefore each eigenvalue in the eigenvalue support of D lies in $\{\theta_r : E_r D \neq 0\}$. If $\nu := \{\theta_r : E_r D \neq 0\}$, we have $r+1 \leq \nu$.

$D = D^{1/2} D^{1/2}$

$E_r D^{1/2} \neq 0$

(b). All eigenvalues of X lie in the interval $[-k, k]$.

Since the difference between distinct eigenvalues of the eigenvalue support is at least one, the size of the eigenvalue support is at most $2k+1$.

(c) $V(X)$ is covered by the s balls of radius r about the vertices in S and consequently

$$|V(X)| \leq s\{1 + k + k(k-1) + \cdots + k(k-1)^{r-1}\}. \qquad \square$$