UChicago REU 2013 Apprentice Program **Spring 2013**

Lecture 17: July 24th, 2013

Prof. Babai Scribe: David Kim

Student Questions: Three Squares Theorem (Redmond); Mantel-Turán (Yujia); $avg\deg \leq \mu_1 \leq max\deg$ (Annie); Aut(Petersen) (Annie, Yujia); $G \not\supseteq C_4 \Rightarrow m \leq cn^{3/2}$ (Redmond).

Prof. Babai: Expander Mixing Lemma; If T (triangular) normal, then diagonal; Cayley-Hamilton Theorem.

1 Problems

1.1 Three Squares Theorem

Theorem 1.1 *$x, y, z \in \mathbb{Z}$ then $x^2 + y^2 + z^2 \neq 8k + 7$.*

Proof: [Proof by *infinite descent*] The claim holds for $k = 0, 1, 2$ (check). So at least one of x, y, z, say x, $x \geq 4$. Suppose $\exists$ smallest k such that $x^2 + y^2 + z^2 = 8k + 7$. But as long as $x \geq 3$, $(x-4)^2 + y^2 + z^2 < x^2 + y^2 + z^2$, but $(x-4)^2 + y^2 + z^2 = 8k' + 7$ for $k' < k$. (contradiction) ■

Lemma 1.2 *(Lemma for a different solution) $a \equiv b \mod m, c \equiv d \mod m \Rightarrow a \pm c \equiv b \pm d \mod m, ac \equiv bd \mod m$. (prove this)*

Proof: [Proof by above Lemma] We can restate the problem as $x, y, z \in \mathbb{Z} \Rightarrow x^2 + y^2 + z^2 \neq 7 \mod 8$. If x is even, $x^2 \equiv 0 \mod 8$ or $x^2 \equiv 4 \mod 8$.

Claim 1.3 *If x is odd, $x^2 \equiv 1 \mod 8$.*

(Proof) $x^2 - 1 = (x+1)(x-1)$. But $x-1$ and $x+1$ are consecutive even numbers, so one of them is a multiple of 4. Therefore, $8|x^2 - 1$. □

Consider all cases of even or odd for each x, y, z, and always $x^2 + y^2 + z^2 \neq 7 \mod 8$ ■

1.2 Four Squares Theorem

Exercise 1.4 *If $a = x^2 + y^2, b = r^2 + s^2 \Rightarrow ab = u^2 + v^2$ $(a, b, x, y, r, s \in \mathbb{Z})$.*
hint: complex numbers

Proof: Let $z = x + iy, w = r + is \Rightarrow z\overline{z} = |z|^2 = x^2 + y^2 = a$, and $w\overline{w} = |w|^2 = r^2 + s^2 = b$. Then $ab = |z|^2|w|^2 = |z \cdot w|^2 = |(xr - ys) + i(yr + xs)|^2 = (xr - ys)^2 + (yr + xs)^2$. ■

So the product of sums of two squares is also a sum of two squares. This implies that if every prime number were to be a sum of two squares, then any nonnegative integer would also be a sum of two squares. (Note: we must permit 0)

Exercise 1.5 *If p is prime and $p = x^2 + y^2 \Leftrightarrow p = 2$ or $p \equiv 1 \mod 4$. It is possible to prove this using Fermat's infinite descent.*

Given any $n = \prod_i p_i^{k_i}$, how can one tell if it is a sum of two squares? Clearly it is sufficient that each $p_i \equiv 1 \mod 4$, but not necessary (counterexample: 9). The following exercise states the necessary and sufficient condition.

Exercise 1.6 $n = \prod_i p_i^{k_i} = x^2 + y^2 \Leftrightarrow (\forall i)(p_i \equiv -1(4) \Rightarrow 2|k_i)$*, i.e. every prime factor that is* $-1 \mod 4$ *has an even power.*

One of the most famous theorems about congruences is the following:

Theorem 1.7 (Fermat's Little Theorem) *If* $\gcd(a, p) = 1$*,* p *prime* $\Rightarrow a^{p-1} \equiv 1 \mod p$.

Note that FLT refers to the following theorem:

Theorem 1.8 (Fermat's Last Theorem (FLT)) *If* $a^n + b^n = c^n, n \geq 3 \Rightarrow abc = 0$ *(no non-zero integer solutions).*

Possibly the single most famous theorem in modern mathematics, Fermat's Last Theorem was proven by Andrew Wiles in 1994. The original proof was found to have a gap, but Wiles managed to fix it - an unusual event in mathematics, as most proofs for famous conjectures usually break down completely when found to contain a gap. In fact, Wiles did not fix the error directly, but took a different approach which allowed him to avoid the original gap.

A proof usually reveals only the most elegant path from the initial conditions to the desired theorem, and the entire "forest" is often hidden. A mathematician builds one's own world of mathematics, and eventually with some luck, finds paths to proofs and theorems which sometimes even become motivations for new fields of study.

Fermat's Last Tango - a musical featuring Fermat, Euclid, Gauss, Newton, Pythagoras, and (fictional) Wiles in the "aftermath." Gauss is portrayed as a jealous character complaining Wiles' use of "20th century math."

Definition 1.9 (Quaternions) *A 4-dimensional vector space over* $\mathbb{R}$ *with basis* $\{1, i, j, k\}$ *(quaternion units), with multiplication of the basis defined as* $i^2 = j^2 = k^2 = -1$*,* $ij = k, jk = i, ki = j$*,* $ji = -k, kj = -i, ik = -j$*. Quaternions are multiplied by distributivity using these rules. In this basis, every element can be expressed as* $w = a + bi + cj + dk$*, the conjugate* $\overline{w} = a - bi - cj - dk$*, and* $|w|^2 = w\overline{w} = a^2 + b^2 + c^2 + d^2$.

Note that quaternions are an extension of the complex numbers, and is similar to a field except for multiplicative commutativity. There is no 3-dimensional division algebra - the quaternions were the first non-commutative division algebra, discovered by Hamilton.

Exercise 1.10 *Prove: the product of two sums of four squares is also a sum of four squares. Answer: use quaternion multiplication -* $|w_1||w_2| = |w_1 \cdot w_2|$.

Therefore, proving the Four Squares Theorem also reduces to proving it for prime numbers. If $p \equiv 1 \mod 4$, we are done by adding two 0's. Prove it for $p \equiv -1 \mod 4$ and you are done.

1.3 Extremal graph theory

Theorem 1.11 (Mantel-Turán) *If $G \not\supseteq K_3 \Rightarrow m \leq \frac{n^2}{4}$.*
hint: induction in steps of two: remove a pair of adjacent vertices to reduce to a smaller case

Proof: Let G' be obtained by deleting any edge $e = (x, y) \in E(G)$ (delete x, y and all adjacent edges). Then $|E(G)| - |E(G')| \leq n-1$, since each $v \neq x, y$ can be adjacent to at most one of x or y (otherwise we have a triangle), and $e \notin E(G')$. So $|E(G)| \leq n-1+|E(G')| \Rightarrow |E(G)| \leq n-1+\frac{(n-2)^2}{4}$ by induction hypothesis, and $|E(G)| \leq \frac{n^2}{4}$. (Similar induction technique works for larger cliques) ■

Exercise 1.12 (Inequality of the arithmetic and quadratic mean) *Prove:* $\frac{x_1 + \cdots + x_n}{n} \leq \sqrt{\frac{x_1^2 + \cdots + x}{n}}$
where the x_i are real.
(hint 1: brute force; hint 2: Cauchy-Schwarz)

Recall the following tricker problem:

Exercise 1.13 (Kővári–Turán–Sós) *If $G \not\supseteq C_4 \Rightarrow m \leq cn^{3/2}$.*

In these kinds of problems, we want to translate a structural combinatorial condition into a simpler counting problem - for this problem, we count walks of length 2.

Proof: Let $S = \{(a, x, b) : a \neq b, a \sim x \sim b\}$. Then $|S| \leq n(n-1)$, since having chosen a and b, we can only have one x (otherwise, we would have a C_4). On the other hand, $|S| = \sum_{x \in V} d_x(d_x - 1)$ - for each x, choose a and b from its neighbors. So we have

$$\begin{aligned} &\sum_x d_x(d_x - 1) \leq n(n-1) \leq n^2 \\ &\Rightarrow \sum_x d_x^2 - \sum_x d_x = \sum_x d_x^2 - 2m \leq n^2 \\ &\Rightarrow \sum_x d_x^2 \leq n^2 + 2m \end{aligned} \tag{1}$$

since $m = \frac{1}{2}\sum_x d_x$. Then by (exercise 1.12) and (1),

$$\begin{aligned} &\frac{4m^2}{n} = \frac{1}{n}\left(\sum_{x \in V} d_x\right)^2 \leq \sum_x d_x^2 \leq n^2 + 2m \\ &\Rightarrow 4m^2 - 2mn = \left(2m - \frac{n}{2}\right)^2 - \frac{n^2}{4} \leq n^3 \end{aligned} \tag{2}$$

Using $n^3 + \frac{n^2}{4} < (n+1)^3$ in (2),

$$\begin{aligned} &2m < \frac{n}{2} + (n+1)^{3/2} \sim n^{3/2} \\ &\Rightarrow m \lesssim \frac{1}{2}n^{3/2} \end{aligned}$$

■

A question that naturally follows: are there examples of equality (tight examples)? Yes.

Exercise 1.14 *(not quite easy) Find infinitely many graphs without C_4 such that $n \geq cn^{3/2}$, $c > 0$ constant.*

1.4 Largest Eigenvalue of an Adjacency Matrix

Exercise 1.15 *Let A be the adjacency matrix of an undirected graph with largest eigenvalue μ_1. Then $avg\deg \leq \mu_1 \leq max\deg$.*

Proof: We first prove the upperbound. Let $Av = \mu_1 v$. Then $v \neq 0$(eigenvector) and we may assume the largest component of v, say $v_i > 0$, since $A(-v) = \mu_1(-v)$. Then $(Av)_i = \sum_{j\sim i} v_j = \mu_1 v_i \leq (max\deg) \cdot (v_i)$ gives us the bound.

We use the Rayleigh quotient for the lower bound. By Courant-Fischer,

$$\forall x \neq 0, R_A(x) = \frac{x^T Ax}{x^T x} \leq \mu_1$$

In particular, for $x = (1, \ldots, 1)^T$, we have

$$R_A(x) = \frac{\sum_{i\in V} \deg i}{n} = avg\deg$$

■

1.5 Triangular and normal, then diagonal

Recall $A \in M_n(\mathbb{C})$ is normal if $AA^* = A^*A$, where A^* is the conjugate transpose of A.

Claim 1.16 *If A is normal and upper triangular $\Rightarrow$ A diagonal.*

Proof: Let $A^*A = B$, $AA^* = C$. Then $B_{11} = a_{11}\overline{a_{11}} = |a_{11}|^2$, $C_{11} = \sum_{i=1}^n |a_{1i}|^2$ by simple matrix multiplications, and since $B_{11} = C_{11}$, $\sum_{i=2}^n |a_{1i}|^2 = 0 \Leftrightarrow |a_{1i}|^2 = 0$ for each $i > 1 \Leftrightarrow a_{1i} = 0$ for each $i > 1$. Recurse on each of the remaining rows, given the results for previous rows. ■

Exercise 1.17 *If $A = A^*$ (self-adjoing, or Hermitian) $\Rightarrow$ all eigenvalues of A are real.*
hint: quadratic form of A

Proof: Assume $Au = \lambda u$, $\lambda \in \mathbb{C}$. Then $Q_A(u) = u^*Au = \lambda||u||^2$. Taking the conjugate transpose, $(u^*Au)^* = \overline{\lambda}||u||^2$. But $(u^*Au)^* = u^*A^*u = u^*Au$ and we have $\lambda||u||^2 = \overline{\lambda}||u||^2$. As u is an eigenvector, $||u||^2 \neq 0$ and $\lambda = \overline{\lambda} \Rightarrow \lambda \in \mathbb{R}$. ■

How do these relate to the Spectral Theorem? Recall Schur's Theorem: $\forall A \in M_n(\mathbb{C}), \exists U$, unitary, such that $U^*AU = T$, where T is upper triangular. So A is *unitarily similar* to an upper triangular matrix, which contains the eigenvalues of A on the diagonals ($f_A = f_T$). What do we know about the first column of U? It must be an eigenvector ($Au_1 = Ut_1 = T_{11}u_1$).

So the chain of logic is: if $A \in M_n(\mathbb{C})$, $A^*A = AA^*$

1. By Schur's Theorem, $A \sim_u T$.
2. Since $AA^* = A^*A, T^*T = TT^*$.
3. Since T is triangular and normal $\Rightarrow T$ is diagonal.

For the real case: If $A = U^T DU$ (orthogonally diagonalizable) $\Leftrightarrow A = A^T$.

- If $A = U^T DU \Rightarrow A^T = U^T D^T U = U^T DU = A$.
- Conversely, if $A = A^T \Rightarrow A$ is normal, so $A \sim D$ by the Spectral Theorem. Also, since the eigenvalues of A are real (exercise 1.17), U is real.

1.6 Matrix-Tree Theorem

Definition 1.18 *The spanning tree of a graph G is a tree inside G which reaches every vertex. Question: given G, how many spanning trees are there?*

Theorem 1.19 (Matrix-Tree Theorem - Kirchhoff 1848) ** Given G and its adjacency matrix A, degree matrix D, let $L = D - A$ be the Laplacian. Then # of spanning trees of $G = \det L'$, where L' is any truncated matrix of L obtained by removing a row and a column (and maybe changing sign). (Note: there is a proof that uses only the definition of the determinant.)*

Exercise 1.20 *If $A \in M_n(\mathbb{R}), A = A^T$, A is positive definite $\Leftrightarrow$ all corner determinants > 0. A corner determinant is the determinant of an upper-left submatrix.*

1.7 Perron-Frobenius Theorem

$A \in M_n(\mathbb{R})$ is non-negative if $(\forall i, j)(a_{ij} \geq 0)$. Likewise, a vector x is non-negative, $x \geq 0$, if $(\forall i)(x_i \geq 0)$.

Exercise 1.21 *If $A \in M_n(\mathbb{R}), A = A^T, A \geq 0 \Rightarrow \exists x \geq 0 (x \neq 0)$ such that $Ax = \lambda x$. (Can you just guess the eigenvalue and the eigenvector?)*

Proof: The largest eigenvalue μ_1 has a nonnegative eigenvector. We know $\mu_1 = \max_{x \neq 0} R_A(x) = \frac{x^T Ax}{x^T x}$. If x were to have negative components, switching the signs does not change the denominator, and does not decrease the numerator for R_A, since $A \geq 0$. Thus, we may assume x is nonnegative for μ_1. ■

Exercise 1.22 (Perron-Frobenius) *If $A \geq 0 \Rightarrow \exists x \geq 0$ eigenvector.*
Note: We cannot use Rayleigh quotients.