Advanced Graph Algorithms Jan-Apr 2014

Lecture 7 — January 20, 2014

Lecturer: Saket Saurabh *Scribe: Anantha Padmanabha MS*

1 Overview

In the last lecture, we studied $nice-tree-decomposition$ and its application to find a dynamic-programming algorithm for solving MIS for a graph with tree width atmost t.

In this class we shall see a few concepts of linear algebra and their applications to solve a few graph related problems.

2 Preliminaries :

Let us first recall some basic definitions

Determinant of a matrix : Determinant of a square matrix $A = [a_ij]_{n\times n}$ is defined as :

$$det(A) = \sum_{\sigma \in S_n} sgn(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

where,

- S_n is the set of all permutations over $\{1....n\}$
- $sgn(\sigma) = (-1)^j$
  where j is the number of inversions in σ (i.e, the number of $i < j$ such that $\sigma(i) > \sigma(j)$)
- $a_{i,j}$ is the entry in the matrix A corresponding to i^{th}s row and j^{th} coloumn.

Example :

- $$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$
$$= sgn([123]) \prod_{i=1}^{3} a_{i,[123](i)} + sgn([132]) \prod_{i=1}^{3} a_{i,[132](i)} + sgn([213]) \prod_{i=1}^{3} a_{i,[213](i)} +$$
$$sgn([231]) \prod_{i=1}^{3} a_{i,[231](i)} + sgn([321]) \prod_{i=1}^{3} a_{i,[321](i)} + sgn([312]) \prod_{i=1}^{3} a_{i,[312](i)}$$

$$= \prod_{i=1}^{3} a_{i,[123](i)} - \prod_{i=1}^{3} a_{i,[132](i)} - \prod_{i=1}^{3} a_{i,[213](i)}$$
$$+ \prod_{i=1}^{3} a_{i,[231](i)} - \prod_{i=1}^{3} a_{i,[321](i)} + \prod_{i=1}^{3} a_{i,[312](i)}$$
$$= a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} - a_{13}a_{22}a_{31} + a_{13}a_{21}a_{32}$$

Rank of a matrix: Rank of a matrix is the maximum number of linearly independent rows of a matrix. It is also equal to the maximum number of linearly independent coloumns of a matrix.

Note :

- The normal matrix multiplication takes running time $O(n^3)$.
- However, algorithms like Strassen's algorithm and Coppersmith-Winograd algorithm take a subcubic order running time.
- Till date, the best-known martix multiplication running time is obtained by Virginia Williams and has $O(n^{2.3727})$
- We shall assume that the matrix multiplication can be achieved in $O(n^\omega)$ where, ω is the index of the best bound for the running time of matrix multiplication.
- Computing rank of a matrix and determinant of a matrix can be done as fast as $O(n^\omega)$.

Polynomial Identity Testing : The problem is to essentially **check whether the input polynomial evaluates to** 0 **on all possible inputs** . In that case, we also say that **the polynomial is identically zero**. If a polynomial p is not identically zero, then it is denoted by $p \not\equiv 0$.

If the polynomial is explicitly expressed in the input, then the running time to determine whether the polynomial is identically zero is polynomial in the length of the input. However if the polynomial is expressed as a circuit or as the determinant of a matrix, then it is not known whether the output can be obtained in the polynomial running time of the length of the input. This problem is known to be in **co-RP**. We consider the case where the input polynomial is specified as determinant of a matrix.

Lemma 1. *Schwartz-Zippel lemma : Let $p(x_1, x_2, \ldots, x_n)$ be a polynomial of total degree d. Assume that p is not identically 0, then if we pick $y_1y_2...y_n$ independently and uniformly over a finite field S, then the probablity:*

$$Pr[p(y_1, y_2, \ldots, y_n) = 0] \leq \frac{d}{|S|}$$

Proof. By indution on n

Base case : When $n = 1$, By Fundamental theorem of algebra, $p(x_1)$ of degree d has atmost

d roots. Hence $Pr[p(y_1) = 0] \leq \frac{d}{|S|}$

Induction step : $n > 1$, Let $p(x_1, x_2, \ldots x_n) = \sum_{i=1}^{d} x_1^i q_i(x_2, x_3, \ldots x_n)$
Since p is not identically 0, for some $k \in [d]$, $q_k \not\equiv 0$.
Degree of $q_k \leq d - k$ because degree of $x_1^k q_k \leq d$.
By induction hypothesis, $Pr[q_k(y_2, y_3, \ldots y_n) = 0] \leq \frac{d-k}{|S|}$
if $q_k(y_2, y_3, \ldots y_n) \not\equiv 0$ then $Pr[p(y_1, y_2, \ldots y_n) = 0 | q_k(y_2, y_3, \ldots, y_n) \not\equiv 0] \leq \frac{k}{|S|}$

Let $E1$ denote $p(y_1 y_2 .. y_n) \equiv 0$ and $E2$ denote $q_k(y_2 y_3 ... y_n) \equiv 0$

$$Pr[E1] = Pr[E1 \text{ and } E2] + Pr[E1 \text{ and } \overline{E2}]$$
$$Pr[E1 \text{ and } E2] = Pr[E1 \cap E2] = Pr[E1|E2] \cdot Pr[E2]$$
$$Also, Pr[E1|E2] = 1$$
$$Hence, Pr[E1] = Pr[E2] + Pr[E1|\overline{E2}] \cdot Pr[\overline{E2}]$$
$$Pr[E1] \leq Pr[E2] + Pr[E1|\overline{E2}]$$
$$Pr[E1] \leq \frac{d-k}{|S|} + \frac{k}{|S|}$$
$$Pr[E1] \leq \frac{d}{|S|}$$

This completes the proof. □

Suppose S is a finite field and p is a monomial of degree d then p can be evaluated at $d+1$ points to decide whether p is identically zero or not. If p is a polynomial of n variables and total degree d, and let x be the total number of solutions to p in S, then by lemma $\frac{x}{|S|^n} \leq \frac{d}{|S|}$.
Hence, $x \leq d \cdot |S|^{n-1}$.

If the input is given in the form of $n \times n$ matrix with each term as a monomial and whose determinant is the input polynomial, then the total degree of the polynomial $\leq n^2$. Suppose $S = \{0, 1, ..k\}$ then the number of roots$(x) \leq n^2 \cdot k^{n^2-1}$, So we can evaluate the determinant of the matrix at $n^2 \cdot k^{n^2-1} + 1$ number of points to decide whether the polynomial is identically zero or not. The running time of this algorithm would be O$(n^2 \cdot k^{n^2} \cdot n^\omega)$

However, if we fix $S = \{1, 2, \ldots n^2\}$ and randomly pick $(x_1, x_2, \ldots, x_n)$ with uniform probablity and evaluate the determinant and it evaluates to non-zero, then the polynomial is non-zero. But the probablity of the polynomial evaluating to 0 when the polynomial is not identically zero would be Pr[error] $\leq \frac{n^2}{2n^2} = \frac{1}{2}$.

If $|S| = 500n^2$ then Pr[error] $\leq \frac{1}{500}$

If $|S| = 2^n \cdot n^2$ then Pr[error] $\leq \frac{1}{2^n}$
With $|S| = 2^n \cdot n^2$ if the same procedure is repeated for p times then Pr[error]$\leq \frac{1}{2^{np}}$

So the probablity of success, Pr[Success] $\geq 1 - \frac{1}{2^{np}}$
The running time of this probablistic algorithm is $O(n^\omega)$ because p is constant. Thus we have an efficient algorithm for Polynomial Identity Testing with a very high prpbablity of success.

3 Recution of Graph problems to PIT :

3.1 Problem 1: Perfect matching in a Bipartite graph

Problem desciption : Given a Bipartite graph $G(X, Y, E)$, Does G has a perfect matching ?

This problem can be reduced to PIT as follows :
In the incidence matrix M [1] of the Bipartite graph, where the rows correspond to the vertices of the partition X and coloumns corresponds to the vertices of the partition Y, replace $M(i, j)$ by x_{ij} iff $M(i, j) = 1$. Let $A[\bar{x}]$ be the new matrix with atmost n^2 variables. This matrix $A[\bar{x}]$ is called Edmond's matrix.

Theorem 2. *G has a perfect matching iff $det(A[\bar{x}]) \not\equiv 0$*

This Theorem will be proved as a corollary of the theorem in the following subsection.

3.2 Problem 2: Perfect matching in a general graph

Problem desciption : Given a graph $G(V, E)$, Does G has a perfect matching ?

This problem can be reduced to PIT as follows :
In the incidence matrix M of the graph, replace $M(i, j)$ by x_{ij} iff $M(i, j) = 1$ and $i < j$ and $M(i, j)$ by $-x_{ij}$ iff $M(i, j) = 1$ and $i > j$. Let $T[\bar{x}]$ be the new obtained matrix. This matrix $T[\bar{x}]$ is called Tuttes matrix.

Theorem 3. *G has a perfect matching iff $det(T[\bar{x}]) \neq 0$*

Proof. $\Rightarrow$:
G has a perfect matching.
This matching can be expressed as a product of disjoint cycles of length 2 where each cycle corresponds to the matches vertices. this will correspond to some permutation σ.
In the determinant expansion, σ is associated with:
$sgn(\sigma) \prod_{i=1}^{n} (x_{i,\sigma(i)})^2 = (-1)^{\frac{n}{2}} sgn(\sigma) \prod_{i=1}^{n} (x_{i,j})^2$

This term will have all variables and hence will not be evaluated to 0. Also, since each term in the permutation is unique, none of the other permutations cancel this term. Hence $\det(T[\bar{x}]) \not\equiv 0$

[1] Incidence matrix : it is a square matrix $A = [a_{ij}]$ for a given graph where the indices of rows and coloums correspond to vertices of the graph and $a_{ij} = 1$ iff there is an edge between i^{th} and j^{th} vertex in the graph.

$\Leftarrow$:
Let, $H = \{\sigma \in S_n | \sigma \text{ has odd length cycle } \}$
Now, $\det(T[\bar{x}]) = \sum_{\sigma \in H} sgn(\sigma) \prod_{i=1}^{n} t_{i,\sigma(i)} + \sum_{\sigma \in (S_n \setminus H)} sgn(\sigma) \prod_{i=1}^{n} t_{i,\sigma(i)}$

Claim : $\sum_{\sigma \in H} sgn(\sigma) \prod_{i=1}^{n} t_{i,\sigma(i)} = 0$
Assuming that the claim is true, it means there is atleast one σ with all even cycles such that the term in the determinant corresponding to σ does not cancel out (because $\det(T[\bar{x}]) \not\equiv 0$. This σ corresponds to a perfect matching where we can pick the alternate edges from all cycles.

Proof of the claim :
Consider a bijection $\psi : H \to H$ where,

- $\psi(x) \neq x$
- $\psi\psi(x) = x$

We show that the contribution from permutation x and permutation $\psi(x)$ cancells out each other in the determinant.
ψ is constructed as follows : For any $\sigma \in H$ among all the odd cycles, pick the one which has a vertex with smallest number. Reverse the direction of this cycle to obtain σ'. Now, $\psi(\sigma) = \sigma'$ and $\psi(\sigma') = \sigma$.

This construction satisfies both the desired conditions. Also, $sgn(x) = sgn(\psi(x))$
Since only the direction of one odd cycle reverses and everything else remains same, x and $\psi(x)$ contributions cancell out each other the expresion obtained for x will be exactly the negative of the expression obtained for$\psi(x)$. Thus these two pairs cancells out each other and hence does not contribute to the determinant.
This completes the proof. □

4 Exercises :

1. Prove that for any matrix, row rank = coloumn rank
2. Prove Theorem 2 as a corollary of Theorem 3.
3. Let A be a real skew-symmetric matrix of dimension n, where n is odd. Then show that $\det(A) = 0$.

$$K = \begin{matrix} \frac{1}{2} & V^t \\ -U & M \end{matrix}$$