4. Finding the Shortest Cycle

Thursday, August 31, 2023 4:37 PM

Thm (Cygan-Gabow-Sankowski): There exists a randomized $\tilde{O}(n^\omega \cdot M)$-time algorithm that finds the shortest cycle of directed $G=(V,E)$ with weight $w: E \to \{1,\dots,M\}$ on $n=|V|$ nodes.

Finding the weight of the shortest cycle:

We first prove a weaker theorem:

Thm: There exists a randomized $\tilde{O}(n^\omega M)$-time algorithm finding the weight of the shortest cycle.

Given the weighted directed graph G, define an $n\times n$ matrix A over the ring $\mathbb{F}[X_{11},\dots,X_{nn},Y]$, where $\mathbb{F}$ is a large enough finite field. $|\mathbb{F}|$ is to be determined later.

$$A(i,j) := \begin{cases} X_{ij}\, Y^{w(i,j)} & \text{if } (i,j)\in E \\ 0 & \text{otherwise} \end{cases} \quad \text{for } 1\le i,j\le n.$$

For a polynomial $f \neq 0$ in Y and possibly in other variables, define

$\text{mindeg}_Y(f)$ = smallest d such that f has a monomial of degree d in Y

$\text{mincoeff}_Y(f)$ = the coefficient of $Y^{\text{mindeg}_Y(f)}$ in f, in the variable Y

i.e. the other variables are viewed as constants.

Example: $f(X,Y) = Y^{10} + 10X^3Y^2 + X$.

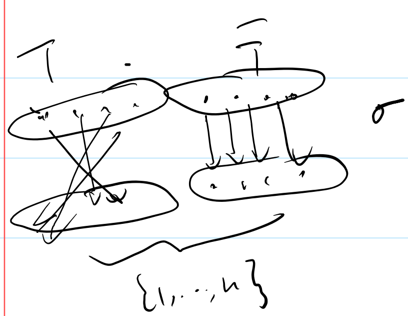
$\text{mindeg}_Y(f) = 0$, since the constant term of f in Y is X.

$\text{mincoeff}_Y(f)$ = coefficient of $Y^0 = 1$ in f $= X$.

Claim: minimum weight of cycles in G = $\text{mindeg}_Y(\det(A+I)-1)$

Proof: By definition,

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



$$= \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \sum_{T \subseteq \{1,\dots,n\}} \prod_{i\in T} A(i,\sigma(i)) \prod_{i \in \bar{T}} I(i,\sigma(i))$$

$$= \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \cdot \sum_{\substack{T \subseteq \{1,\dots,n\} \\ \sigma \text{ fixes } i \text{ for} \\ \text{all } i \in \bar{T}}} \prod_{i \in T} A(i,\sigma(i))$$

Setting $\sigma = \mathrm{id}$ and $T = \phi$ corresponds to the term 1 in $\det(A+I)$.

For each σ and T such that σ fixes all $i \in \bar{T}$, $\prod_{i\in T} A(i,\sigma(i))$ is a monomial in X_{ij} and Y such that its degree in Y is the total weight of cycles in $\sigma|_T$.

Other than the case $\sigma = \mathrm{id}$ and $T = \phi$, the degree of Y in $\prod_{i\in T} A(i,\sigma(i))$ is minimized if $\sigma|_T$ is a single cycle.

This is b/c if $\sigma|_T$ is not, we can replace T by a proper subset to lower the degree of Y (or the total weight of cycles).

The monomials $\prod_{i\in T} A(i,\sigma(i))$ are different if (σ, T) are different.

So no cancellation occurs. This proves the claim. $\square$

It is known that computing the determinant of an $n\times n$ matrix $\Rightarrow$ matrix multiplication.

<u>Thm</u> (Storjohann): If A be an $n\times n$ matrix over $\mathbb{F}[Y]$ where $A(i,j) \in \mathbb{F}[Y]$ has degree $\le M$ for all $1 \le i,j \le n$. Then $\det(A)$ can be computed by an algebraic circuit C over $\mathbb{F}$ of size $\tilde{O}(n^\omega M)$, which can be computed in time $\tilde{O}(n^\omega M)$.

Lemma (Schwartz-Zippel): Suppose $f \in \mathbb{F}[x_1, \dots, x_n]$ has degree $\le d$ ...

Lemma (Schwartz-Zippel): Suppose $f \in \mathbb{F}[x_1, \dots, x_n]$ has degree $\le d$ and $S \subseteq \mathbb{F}$ is a finite set, then

$$\Pr_{(a_1,\dots,a_n) \sim S^n}[f(a_1,\dots,a_n) \neq 0] \geq 1 - \frac{d}{|S|}.$$

Algorithm computing the minimum weight of cycles in G:

Construct a finite field $\mathbb{F}$ of size $\geq n/\varepsilon$, where $\varepsilon > 0$.

Randomly choose $a_{11}, \dots, a_{nn} \in \mathbb{F}$.

Let $\bar{A} = A|_{x_{ij} = a_{ij},\, 1 \le i,j \le n} \in \mathbb{F}[Y]^{n \times n}$.

Compute $\det(\bar{A} + I) - 1$ in the $\tilde{O}(n^\omega M)$ using Storjohann's Thm.

Note $\det(\bar{A}+I) - 1 = \left(\det(A+I)-1\right)(a_{11}, \dots, a_{nn}, Y)$

with prob. $\geq 1 - \frac{n}{|\mathbb{F}|} \geq 1 - \varepsilon$, the coefficient of $Y^{\operatorname{mindeg}_Y(\det(A+I)-1)}$ is nonzero.

In this case, the minimum weight of cycles $= \operatorname{mindeg}_Y(\det(A+I)-1)$ can be found as $\operatorname{mindeg}_Y(\det(\bar{A}+I)-1)$, where $\det(\bar{A}+I) - 1 \in \mathbb{F}[Y]$.

Algorithms computing the shortest cycle:

Claim: (u,v) is in a shortest cycle iff $\dfrac{\partial \operatorname{mincoeff}_Y(\det(A+I)-1)}{\partial x_{u,v}} \neq 0$

Pf: $\operatorname{mincoeff}_Y(\det(A+I)-1) = \sum_{\text{shortest cycle } C} (\pm 1) \cdot \prod_{(u,v) \in C} x_{uv}.$

Different shortest cycles containing (u,v) corresponds to different monomials in $\operatorname{mincoeff}_Y(\det(A+I)-1)$, and hence to different monomials in its partial derivative with respect to x_{uv}. $\square$

From the circuit computing $\det(\bar{A}+I)-1$, we can get a circuit computing $\operatorname{mincoeff}(\det(\bar{A}+I)-1)$ since we know $\operatorname{mindeg}(\bar{A}+I)$

Algorithm: in the algebraic circuit computing $\mathrm{min\,coeff}(\det(\bar{A}+I)-1)$ given $\bar{A}$, for $1 \le i, j \le n$, replacing the $M+1$ input variables specifying the coefficients of $y^0, \dots, y^M$ in $\bar{A}(i,j)$ by the coefficients of $y^0, \dots, y^M$ in $A(i,j)$, which are either zero or X_{ij}.

Then we get an algebraic circuit computing $\mathrm{min\,coeff}(\det(A+I)-1)$

Apply Baur-Strassen to get an algebraic circuit computing

$$\frac{\partial\, \mathrm{min\,coeff}(\det(A+I)-1)}{\partial X_{u,v}} \quad \text{for } 1 \le u, v \le n$$

Choose random assignments $a = (a_{u,v}) \in \mathbb{F}^{n \times n}$.

Then for each (u,v) in a shortest cycle, $\frac{\partial\, \mathrm{min\,coeff}(\det(A+I)-1)}{\partial X_{u,v}}(a)$ is nonzero with probability $\ge 1 - \frac{n}{|\mathbb{F}|} \ge 1-\varepsilon$.

Find $(u,v) \in E$ such that $\frac{\partial\, \mathrm{min\,coeff}(\det(A+I)-1)}{\partial X_{u,v}}(a) \ne 0$

Use Dijkstra to find a shortest path $v \to u$. $\square$

Remark: The assumption $w(i,j) \in \{1, \dots, M\}$ may be relaxed to $w(i,j) \in \{-M, \dots, M\}$.