March 3, 2021 9:19 AM

More Sampling-Based Techniques

I. Witness Finding

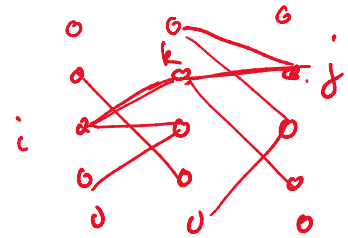
Problem (Boolean matrix multiplication) (BMM)

Given $n \times n$ Boolean matrices A, B,

compute $c_{ij} = \bigvee_{k=1}^{n} (a_{ik} \wedge b_{kj})$

Rmk: related to all-pairs shortest paths (APSP)

e.g. tripartite case



$\forall i, j$, decide if $\exists$ path from i to j of length 2

(Seidel '90: reduce APSP in unweighted undir graphs to BMM)

trivial algm: $O(n^3)$ time

reduces to standard matrix mult. $c'_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$

$(c'_{ij} > 0 \iff c_{ij} = \text{true})$

Strassen '69: $O(n^{2.81})$ time

⋮

Coppersmith, Winograd '90: $O(n^{2.38})$ time

⋮

Le Gall '14: $O(n^{2.37287})$

Alman, Vassilevska W. '21: $O(n^{2.37286})$

let complexity of matrix mult. be $M(n) \approx n^{\omega}$

(ω = matrix mult. exponent)

let complexity of matrix mult. be $M(n) \le n^{\omega}$
(ω = matrix mult. exponent)

But if c_{ij} true, how to find k ← called a witness
with $a_{ik} \wedge b_{kj}$ true?

Obs For witnesses that are unique,
can find witnesses in $\tilde{O}(M(n))$ time.

Pf 1: Compute $\hat{c}_{ij} = \sum_{k=1}^{n} \underbrace{k\, a_{ik}}_{\hat{a}_{ik} = k a_{ik}} b_{kj}$. ← $\square$

Pf 2: fix $\ell \le \log n$.

Compute $c_{ij}^{(\ell)} = \bigvee_{k:\ \ell^{th} \text{ bit of } k \text{ is } 1} (a_{ik} \wedge b_{kj})$ ←

$c_{ij}^{(\ell)}$ true $\iff$ ℓ^{th} bit of witness for c_{ij} is 1.

$\Rightarrow$ $O(M(n) \log n)$ time. $\square$

But how to ensure uniqueness?

idea - take rand sample R of diff. sizes

Lemma Fix $W \subseteq \{1, \dots, n\}$.
Pick rand sample $R \subseteq \{1, \dots, n\}$ of size r.
If $\frac{n}{4|W|} \le r \le \frac{n}{2|W|}$, $\quad \frac{n}{4r} \le |W| \le \frac{n}{2r}$
then $\Pr[|W \cap R| = 1] \ge \Omega(1)$.

Pf: Let $x_1, \dots, x_r$ be r rand. elems in $\{1, \dots, n\}$.

Pf: Let $x_1, \dots, x_r$ be r rand. elems in $\{1, \dots, n\}$.

$$\Pr[\text{exactly one of } x_1, \dots, x_r \text{ is in } W]$$

$$= \Pr[\text{at least one of } x_1, \dots, x_r \text{ is in } W] - \Pr[\text{at least two } \dots\dots]$$

$$\geq r \cdot \frac{|W|}{n} - r^2 \left(\frac{|W|}{n}\right)^2$$

$$\geq \frac{1}{4} - \left(\frac{1}{4}\right)^2 = \Omega(1).$$

$x - x^2$
$x \in [\frac{1}{4}, \frac{1}{2}]$

$\square$

Note - pairwise indep. ...

Sol'n - use sample $R^{(\ell)}$ of size 2^ℓ, $\ell = 1, \dots, \log n$

(Alon, Galil, Margalit '97) find witness of $\bar{c}_{ij}^{(\ell)} = \bigvee_{k \in R^{(\ell)}} (a_{ik} \wedge b_{kj})$

repeat $O(\log n)$ times to get high prob.

$\Rightarrow$ total time $\boxed{\tilde{O}(M(n) \log^2 n)}$

Rmk - derandomize? Alon-Naor '96

II. Color Coding

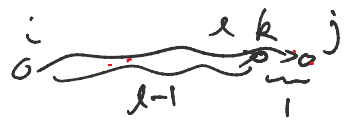
Problem Given dir. graph G & small int. k, decide if G contains a simple cycle of length k exactly.

(NP-hard when k is large)

Attempt 1 - by matrix mult. (or DP)

let $A = (a_{ij})_{ij}$ be adj matrix

let $a_{ij}^{(\ell)} = \begin{cases} 1 & \text{if } \exists \text{ non-simple path from } i \text{ to } j \text{ of length } \ell \\ 0 & \text{else} \end{cases}$



$$a_{ij}^{(\ell)} = \underbrace{\bigvee_{k=1}^{n} \left(a_{ik}^{(\ell-1)} \wedge a_{kj} \right)}_{\text{Boolean MM: } A^{(\ell)} = A^{(\ell-1)} \cdot A}$$

$\Rightarrow O(k n^{\omega})$ time

improves to $O(n^{\omega} \log n)$ by repeated squaring

$$A^{(\ell)} = A^{(\ell/2)} \cdot A^{(\ell/2)}$$

G has non-simple cycle of length k iff $\exists\, ij \in E$ with $a_{ji}^{(k-1)} = 1$.

But cycle may not be simple!

idea - (Alon, Yuster, Zwick '95)

divide V into k rand. subsets

more precisely,

for each $v \in V$,

pick rand. $h(v) \in \{1, \dots, k\}$ (indep'ly)

"color" of v

Def A k-cycle C is <u>colorful</u> if all k vertices have diff. colors.

$\Rightarrow$ colorful k-cycles are automatically simple

$\Rightarrow$ colorful k-cycles are automatically simple

Can decide if $\exists$ colorful k-cycle by matrix mult. & repeated squaring.

For each subset $\underline{S} \subseteq \{1,\dots,k\}$,

$$a_{ij}^{(S)} = \begin{cases} 1 & \text{if } \exists \text{ path of length } |S| \text{ using precisely the colors in } S \\ 0 & \text{else} \end{cases}$$

$$a_{ij}^{(S)} = \bigvee_{\substack{T \subseteq S \text{ of} \\ \text{size } |S|/2}} \left(a_{ik}^{(T)} \wedge a_{kj}^{(S-T)} \right)$$

$\Rightarrow \quad O(2^k n^\omega \log n)$ time

G has colorful k-cycle iff $\exists\, ij \in E$ with $a_{ji}^{\{1,\dots,k\}} = \text{true}$.

Lemma For a fixed k-cycle C,

$$\Pr[\, C \text{ is colorful} \,] \geq \frac{1}{e^k} =: p$$

Pf: Say $C = u_1 \cdots u_k u_1$.

$$\Pr[\, h(u_1), \dots, h(u_k) \text{ is a permutation of } \underline{1,\dots,k} \,]$$

$$= \frac{k!}{k^k}$$

$$\approx \frac{\overset{k^k}{\sqrt{2\pi k}\left(\frac{k}{e}\right)^k}}{k^k} \approx \frac{1}{e^k}. \quad \square$$

repeat $\sim \frac{c}{p}\log n$ times

$\Rightarrow$ err prob. $(1-p)^{\frac{c}{p}\log n} \sim e^{-p\frac{1}{p}\log n}$

$= 1/n^c.$

$\Rightarrow$ total time

$$\tilde{O}\left(\frac{1}{p}\cdot 2^k n^\omega\right)$$

$$= \tilde{O}\left((2e)^k n^\omega\right) \text{ time}$$

$$\lesssim \boxed{\tilde{O}\left(\underline{5.44}^k n^\omega\right)}$$

(Monte Carlo)