- For any two boolean matrices $A_{n \times n}$ and $B_{n \times n}$, we call $k$ a witness of tuple $(i, j)$ whenever $A_{i k}=B_{k j}=$ 1. A matrix $W_{n \times n}$ is called a witness matrix of boolean matrices $A_{n \times n}$ and $B_{n \times n}$ whenever $W_{i j}$ stores a witness corresponding to tuple $(i, j)$ for every $1 \leq i, j \leq n$. The witness matrix has many applications, including efficiently computing all-pairs shortest paths in unweighted undirected graphs and transitive closure of directed graphs.
- The $i j$-th entry of $A B$, denoted by $[A B]_{i j}$, has the number of witnesses of tuple $(i, j)$.

First, we devise an algorithm to find the witness of those $(i, j)$-entries of $W$ for which there is exactly one witness; that is, for such $(i, j)$ tuple, there is only one $k$ such that $A_{i k}=B_{k j}=1$. Later, with the help of random sampling, this algorithm is extended to find every entry of $W$.

- Lemma 1: Let $A_{n \times n}^{\prime}$ be a matrix with $A_{i j}^{\prime}=j A_{i j}$ for every $1 \leq i, j \leq n$. For any $(i, j)$, if $[A B]_{i j}=1$, then $\left[A^{\prime} B\right]_{i j}$ has the unique witness of $(i, j)$.

Proof: If $[A B]_{i j}=1$, then there exists a $k$ such that $A_{i k}=1$ and $B_{k j}=1$. That is, $k$ is the witness for $[A B]_{i j}$ being equal to 1 , and for every $k^{\prime} \neq k$, either $A_{i k^{\prime}}=0$ or $A_{k^{\prime} j}=0$. Hence, $\left[A^{\prime} B\right]_{i j}=$ $\sum_{k=1}^{n} A_{i k}^{\prime} B_{k j}=k$.

- Using this observation, the following deterministic algorithm finds the correct witness for every $(i, j)$ that has a unique witness:
(a) for every $1 \leq i, j \leq n$
(b)

$$
A_{i j}^{\prime}=j A_{i j}
$$

(c) compute $A^{\prime} B$ and $A B$
(d) for every $1 \leq i, j \leq n$

$$
\begin{equation*}
\text { if }[A B]_{i j} \text { is equal to } 1 \text { then } W_{i j}=\left[A^{\prime} B\right]_{i j} \text { else } W_{i j}=0 \tag{e}
\end{equation*}
$$

- For a tuple $(i, j)$, let $w=[A B]_{i j}>2$. That is, $w$ is the number of witnesses for tuple $(i, j)$. We show that a random sample $R \subseteq[n]$, with $\frac{n}{2} \leq w|R| \leq n$, is very likely to have a witness for $(i, j)$.
Next we define matrices $A^{R}$ and $B^{R}$. For any $k \in[1, n]$ not in $R$, we define the $k^{t h}$ column of $A^{R}$ and the $k^{\text {th }}$ row of $B^{R}$ are null vectors; if $k \in R$, then $k^{\text {th }}$ column in $A^{R}$ is same as the $k^{\text {th }}$ column in $A$ and $k^{\text {th }}$ row in $B^{R}$ is same as the $k^{t h}$ row in $B$. First, this construction leads to $i j$-th entry of $\left[A^{R} B^{R}\right]$ to have the unique witness when $(i, j)$ has a unique witness. Further, the following theorem shows random sampling could help in finding a witness of $(i, j)$ if $(i, j)$ has more than one witness.

Theorem 1: For any $(i, j)$, given $[A B]_{i j}=w>0$, the probability $\left[A^{R} B^{R}\right]_{i j}=1$ is at least $\frac{1}{2 e}$.
Proof: This probability is

$$
\begin{aligned}
& =\frac{\binom{w}{1}\binom{n-w}{\mid R-1-1}}{\left(\begin{array}{l}
n \mid
\end{array}\right)} \\
& =\frac{w|R|}{n}\left(\Pi_{j=0}^{w-2} \frac{n-|R|-j}{n-1-j}\right) \\
& \geq \frac{w|R|}{n}\left(\Pi_{j=0}^{w-2} \frac{n-|R|-j-(w-j-1)}{n-1-j-(w-j-1)}\right)
\end{aligned}
$$

$$
\begin{aligned}
& =\frac{w|R|}{n}\left(\Pi_{j=0}^{w-2} \frac{n-w-(|R|-1)}{n-w}\right) \\
& =\frac{w|R|}{n}\left(1-\frac{|R|-1}{n-w}\right)^{w-1} \\
& \geq \frac{1}{2}\left(1-\frac{1}{w}\right)^{w-1 \quad\left(\text { since } \frac{n}{2} \leq w|R| \leq n, \frac{w|R|}{n} \geq \frac{1}{2} \text { and } \frac{|R|-1}{n-w}=\frac{|R|-1}{w\left(\frac{n}{w}-1\right)} \leq \frac{1}{w}\right)} \\
& \geq \frac{1}{2 e}
\end{aligned}
$$

- For any entry $[A B]_{i j}$, if there are many witnesses, then having a small $|R|$ helps. On the other hand, if $[A B]_{i j}$ has small number of witnesses, then having a large $|R|$ would help. Hence, every size in $S=\left\{1,2, \ldots \frac{n}{2}\right\}$ is tried for $|R|$. Speicifically, for $w=[A B]_{i j}$, there exists a $|R| \in S$ satisfying $\frac{n}{2} \leq w|R| \leq n$. Besides, as argued below, trying these values for $|R|$ suffice to ensure there will only be a few entries of $W$ left to be computed via brute-force.

For every $d \in S$, repeatedly sampling $R$ of size $d$ independently and uniformly at random from [ $n$ ] for $O(\lg n)$ times, further reduces the probability an entry of $W$ left empty. That is, from Theorem 1 , the probability none of these $R$ vectors lead to a unique witness for $(i, j)$-th entry is at most $\left(1-\frac{1}{2 e}\right)^{O(\lg n)}$, for any $(i, j)$. Of course, witnesses for some of the entries may not be found via this clever idea; these missing witnesses can be found by brute-force.
(a) $C \leftarrow A B$; initialize $W$ to null matrix
(b) for every $d \in S$
(c) repeat for $c \cdot(\lg n)$ times $/ /$ value of $c$ to be fixed later
(d) choose a subset $R \subseteq[n]$ of size $d$, independently and uniformly at random
(e) construct $A^{R}, B^{R}$, and $A^{R m o d}$, where $\left[A^{R m o d}\right]_{i j}$ is $j\left[A^{R}\right]_{i j}$ for every $i, j$ $C^{R} \leftarrow A^{R} B^{R} ; Z \leftarrow A^{R m o d} B^{R}$ for every $1 \leq i, j \leq n$

$$
\begin{equation*}
\text { if } C_{i j}>0 \text { and } C^{R}=1 \text { then } W_{i j} \leftarrow Z_{i j} \tag{g}
\end{equation*}
$$

(i) for every $(i, j)$, if $C_{i j}>0$ and $W_{i j}=0$, find a witness of $(i, j)$ by brute-force

- For any $C_{i j}$, there exists a $d \in S$ such that $\frac{n}{2} \leq C_{i j} \cdot d \leq n$. From the above description, probability that a random choice of $R$ does not have a unique witness for $W_{i j}$ is at most $\left(1-\frac{1}{2 e}\right)$. Hence, probability $W_{i j}$ not found after $c \cdot \lg n$ iterations is at most $\left(1-\frac{1}{2 e}\right)^{c \lg n}$. For having the error probability polynomially small, upper bounding $\left(1-\frac{1}{2 e}\right)^{c \lg n}$ with $\frac{1}{n}$, leads to 3.77 being a lower bound on $c$.

Since the probability an entry of $W$ not found after $c \cdot \lg n$ iterations is at most $\frac{1}{n}$, by the time algorithm reaches step (i), the expected number of witnesses remaining to be found is $n$. Since each entry of $W$ can be determined in $O(n)$ time by brute-force, step (i) takes $O\left(n^{2}\right)$ expected time.

Step (f) takes $O(M M(n))$ time, where $M M(n)$ denotes time to multiply two $n \times n$ matrices, and this step gets executed $O\left((\lg n)^{2}\right)$ times. Steps $(\mathrm{g})-(\mathrm{h})$ take $O\left(n^{2}\right)$ time and they get executed $O\left((\lg n)^{2}\right)$ times. As a whole, the algorithm takes $O\left(M M(n)(\lg n)^{2}\right)$ expected time.

## References:

R. Motwani and P. Raghavan, Randomized Algorithms. Cambridge University Press, 1995.

