Theorem (Tropp)

- $S_1, S_2, \ldots$ nezávislé matice s dim. $d_1 \times d_2$
- $\mathbb{E} S_k = 0$
- $\| S_k \| \leq L$

$\Big\} \; \forall k$

Pak $$\mathbb{E} \Big\| \sum_k S_k \Big\| \leq \sqrt{2 \nu \log(d_1 + d_2)} + \frac{1}{3} L \log(d_1 + d_2),$$

kde $$\nu := \max \Big\{ \Big\| \sum_k \mathbb{E}(S_k S_k^*) \Big\|, \Big\| \sum_k \mathbb{E}(S_k^* S_k) \Big\| \Big\}.$$

Randomizované maticové násobení

- Nechť $B \in \mathbb{R}^{d_1 \times N}$, $C \in \mathbb{R}^{N \times d_2}$ (komplexní lze také)

- Klasické maticové násobení

$$(BC)_{ik} = \sum_{j=1}^{N} b_{ij} c_{jk} \quad ; \quad i = 1, \dots, d_1, \quad j = 1, \dots, d_2$$

Celkem tedy $O(N d_1 d_2)$ operací (sčítání & násobení je jedna operace)

- ! Existují klasické (= deterministické) algoritmy, které jsou rychlejší!

Pro $n = N = d_1 = d_2$ ... $O(n^3)$ ... výše

Strassen $O(n^{2.8074})$ ... 1969

Coppersmith & Winograd $O(n^{2.375477})$ ... 1990

... poslední ... $O(n^{2.3728639})$ ... 2014

} technicky velké konstanty

- Nechť b_j jsou sloupce B a c^j řádky C ... $b_j \in \mathbb{R}^{d_1}$, $c^j \in \mathbb{R}^{d_2}$, $j \in \{1, \dots, N\}$

Pak $b_j \in \mathbb{R}^{d_1 \times 1}$, $c^j \in \mathbb{R}^{1 \times d_2}$

$$(b_j c^j)_{uv} = (b_j)_u (c^j)_v = b_{uj} c_{jv}$$

$$(BC)_{ik} = \sum_{j=1}^{N} b_{ij} c_{jk} = \sum_{j=1}^{N} (b_j c^j)_{ik}$$

V tomto smyslu tedy $BC = \sum_{j=1}^{N} b_j c^j$

- Položme $p_j := \dfrac{\|b_j\|_2^2 + \|c^j\|_2^2}{\|B\|_F^2 + \|C\|_F^2}$ pro $j = 1, 2, \dots, N$

- Zjevně $\sum_{j=1}^{N} p_j = \dfrac{1}{\|B\|_F^2 + \|C\|_F^2} \left(\sum_{j=1}^{N} \left[\|b_j\|_2^2 + \|c^j\|_2^2 \right] \right) = 1$

výpočet p_j: $N d_1 + N d_2$

- Náhodná matice $R = \frac{1}{p_j} b_j c^j$

$$\mathbb{E} R = \sum_{j=1}^{N} p_j \left[\frac{1}{p_j} b_j c^j \right] = \sum_{j=1}^{N} b_j c^j = BC$$

- Vezmeme $\overline{R}_m = \frac{1}{m} \sum_{k=1}^{m} R_k$, R_k jsou nezávislé kopie R

- Chceme odhadnout $\mathbb{E} \| \overline{R}_m - BC \|$ v operátorové normě

Cíl: Použijeme maticové nerovnosti & zformulujeme větu

- $S_k := \frac{1}{m} R_k - \frac{1}{m} BC \quad \dots \quad \sum_{k=1}^{m} S_k = \frac{1}{m} \sum_{k=1}^{m} R_k - BC = \overline{R}_m - BC$

- $\mathbb{E} S_k = \frac{1}{m} \mathbb{E} R_k - \frac{1}{m} BC = 0$

- $\| S_k \| = \| \frac{1}{m} R_k - \frac{1}{m} BC \| \leq \frac{1}{m} \| R_k \| + \frac{1}{m} \| BC \|$

   - $\| R \| \leq \max_j \frac{1}{p_j} \| b_j c^j \| = \max_j \frac{\| b_j \|_2 \cdot \| c^j \|_2}{p_j}$

$$= \max_j \frac{\| b_j \|_2 \cdot \| c^j \|_2}{\| b_j \|_2^2 + \| c^j \|_2^2} \cdot \left(\| B \|_F^2 + \| C \|_F^2 \right)$$

$$\sqrt{\alpha\beta} \leq \sqrt{\frac{\alpha^2 + \beta^2}{2}}$$

$$\frac{\alpha\beta}{\alpha^2 + \beta^2} \leq \frac{1}{2}$$

$$\leq \frac{1}{2} \left(\| B \|_F^2 + \| C \|_F^2 \right)$$

Pro jednoduchost $\| B \| = \| C \| = 1$: $\quad \text{srank}(B) = \frac{\| B \|_F^2}{\| B \|^2}$

$$= \frac{1}{2} \left(\| B \|^2 \cdot \text{srank}(B) + \text{srank}(C) \cdot \| C \|^2 \right)$$

$$= \frac{1}{2} \left(\text{srank}(B) + \text{srank}(C) \right)$$

$$=: \text{asr}(B, C).$$

• Dále $\frac{1}{m}\|BC\| = \frac{1}{m}\|\sum' p_j(\frac{1}{p_j} b_j c^j)\|$

$$\leq \frac{1}{m}\sum_j' p_j \|\frac{1}{p_j} b_j c^j\| \leq \frac{1}{m}\sum' p_j \cdot \max_j \|\frac{1}{p_j} b_j c^j\|$$

$$\leq \frac{1}{m}\cdot \underline{1}\cdot asr(B,C)$$

• Celkem $\|S_k\| \leq \frac{2asr(B,C)}{m}$. $=: L$

|Věta| $\Rightarrow$ $\mathbb{E}\|\sum_k S_k\| = \mathbb{E}\|R_m - BC\| \leq \sqrt{2\nu \log(d_1+d_2)} + \frac{1}{3}L\log(d_1+d_2)$

• $\nu = \max\{\|\sum_{k=1}^m \mathbb{E}(S_k S_k^*)\|; \|\sum_{k=1}^m \mathbb{E}(S_k^* S_k)\|\}$

$$= m\cdot\max\{\|\mathbb{E}(S_1 S_1^*)\|, \|\mathbb{E}S_1^* S\|\}$$

$$0 \preccurlyeq \mathbb{E}(S_1 S_1^*) = \frac{1}{m^2}\mathbb{E}\{[R-BC][R-BC]^*\}$$

$$= \frac{1}{m^2}\{\mathbb{E}(RR^*) - BC(\mathbb{E}R^*) - (\mathbb{E}R)(BC)^* + BC(BC)^*\}$$

$$= \frac{1}{m^2}\{\mathbb{E}(RR^*) - (BC)(BC)^*\} \preccurlyeq \frac{1}{m^2}\mathbb{E}(RR^*)$$

• $\nu \leq \max\{\|\mathbb{E}(RR^*)\|, \|\mathbb{E}(R^*R)\|\}\cdot\frac{1}{m}$

• $\mathbb{E}(RR^*) = \sum_{j=1}^N p_j \frac{(b_j c^j)(b_j c^j)^*}{p_j^2} = \sum_{j=1}^N \frac{1}{p_j}\cdot\|c^j\|^2\cdot b_j b_j^T$

$$= \sum_{j=1}^N \frac{\|B\|_F^2 + \|C\|_F^2}{\|b_j\|_2^2 + \|c^j\|_2^2}\cdot\|c^j\|^2\cdot \underbrace{b_j b_j^T}_{\succcurlyeq 0}$$

$b_j = b,\ c_j = c^T \dots bc^T(bc^T)^T = bc^T c^* b^T = \|c\|^2 \cdot bb^T$

$$\preccurlyeq (\|B\|_F^2 + \|C\|_F^2)\cdot\sum_{j=1}^N b_j b_j^T \preccurlyeq (\|B\|_F^2 + \|C\|_F^2)\cdot BB^*$$

Celkem $v \leq \frac{1}{m}\left(\|B\|_F^2 + \|C\|_F^2\right) \cdot \max\{\underbrace{\|BB^*\|}_{\leq 1}, \underbrace{\|C^*C\|}_{\leq 1}\}$

$$\leq \frac{1}{m} \cdot 2 \cdot asr(B,C).$$

$$\Rightarrow \mathbb{E}\|\bar{R}_m - BC\| \leq \sqrt{\frac{4asr(B,C)}{m}\log(d_1+d_2)} + \frac{1}{3}\cdot\frac{2asr(B,C)}{m}\log(d_1+d_2)$$

Věta: Pro $m \geq \varepsilon^{-2} asr(B,C)\log(d_1+d_2)$ je

$$\sqrt{\frac{4asr(B,C)\log(d_1+d_2)}{m}} \leq \sqrt{\frac{4\varepsilon^2 m}{m}} = 2\varepsilon$$

a $\frac{1}{3}\cdot\frac{2asr(B,C)\log(d_1+d_2)}{m} \leq \frac{2}{3}\,\frac{m\varepsilon^2}{m} = \frac{2}{3}\varepsilon^2$

a tedy $\mathbb{E}\|\bar{R}_m - BC\| \leq 2\varepsilon + \frac{2}{3}\varepsilon^2.$ ∎