# Matrix Completion

Předpokládejme, že $A \in \mathbb{R}^{n\times n}$ je matice s nízkou hodností ($\mathrm{rank}(A) = r \ll n$).

Z této matice pozorujeme jen část ... $\{X_1, \dots, X_{n^2}\}$ je ortonormální báze $(\mathbb{R}^{n\times n}, \|\cdot\|_F)$ a

$$A = \sum_{a=1}^{n^2} \langle X_a, A\rangle_F \cdot X_a \qquad (*)$$

My pozorujeme jen $\{\langle X_a, A\rangle_F\}_{a\in\Omega}$, kde $\Omega \subset \{1,\dots,n^2\}$

Pokusíme se rekonstruovat A z této informace ...

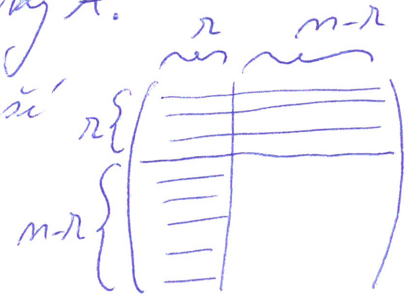
$$\operatorname*{argmin}_{Z\in\mathbb{R}^{n\times n}} \|Z\|_* \text{ s.t. } \langle X_{\omega_j}, Z\rangle_F = \langle X_{\omega_j}, A\rangle_F \qquad (P_*)$$

$j = 1,\dots,m$; $\Omega = \{\omega_1,\dots,\omega_m\}$

Poznámky:
- A budeme předp. samoadj; $X_a$ obecně ne
- $X_i$'s tvaru $e_k \cdot e_l^T$ ... matice s 1 na místě $(k,l)$, 0 jinde, $k,l = 1,\dots,n$

  $\langle X_i, A\rangle_F = \langle e_k \cdot e_l^T, A\rangle = A_{k,l}$

  ... vidíme jen některé prvky A.
- chceme ~~A~~ m co nejmenší




l.b. $\to$ $r\cdot n + (n-r)\cdot r = 2rn - r^2$ parametrů

- $\|Z\|_* = \sum_{j=1}^{n} |\lambda_j(Z)|$ je nukleární norma

Označíme: • Pro $\omega = 1, \dots, n^2$ je $X_\omega$ jeden prvek báze

• Pro $\omega$ náh. veličinu s rovnoměrným rozdělením v $\{1, \dots, n^2\}$

je $X_\omega$ náh. matice a

$$P_\omega : Z \to \langle X_\omega, Z \rangle_F \, X_\omega$$

je náhodný operátor … náhodná projekce

• Vybereme-li $m$ náh. členů (nezávisle, s opakováním) z $(*)$,

dostaneme
$$R : Z \to \frac{n^2}{m} \sum_{j=1}^{m} \langle X_{\omega_j}, Z \rangle_F \, X_{\omega_j}$$

$$\mathbb{E}\, R(Z) = n^2 \cdot \mathbb{E} \langle X_\omega, Z \rangle X_\omega = n^2 \cdot \sum_{k=1}^{n^2} \frac{1}{n^2} \cdot \langle X_k, Z \rangle X_k = Z$$

• Úloha je zjevně neřešitelná např. pro $A = e_1 e_1^T$ & $X$'s typu $\{e_k e_l^T\}_{k,l=1}^{n}$

• $A u_j = \lambda_j u_j$ ; $\lambda_1, \dots, \lambda_r \neq 0$ , $\lambda_{r+1}, \dots, \lambda_n = 0$

$U = \mathrm{range}(A) = \mathrm{span}\{u_1, \dots, u_r\}$ … $A = P_U A = A P_U$
$= \ker(A)^\perp$ $\qquad$ $0 = P_{U^\perp} A = A P_{U^\perp}$

• $Z = (P_U + P_{U^\perp}) Z (P_U + P_{U^\perp})$

• $T := \{ Z : P_{U^\perp} Z P_{U^\perp} = 0 \}$

$P_T$ … projekce na $T$ … $P_T(Z) = P_U Z P_U + P_U Z P_{U^\perp} + P_{U^\perp} Z P_U$
$$= P_U Z + Z P_U - P_U Z P_U$$

**Definice:** Matice $A \in \mathbb{R}^{n \times n}$ s rank$(A) = r$ má koherenci $\nu > 0$ vzhledem k bázi $\{X_a\}_{a=1}^{n^2}$ pokud buď

$$\max_a \|X_a\|^2 \leq \frac{\nu}{n} \qquad (K1)$$

nebo

$$\max \|P_T X_a\|_F^2 \leq \frac{2\nu r}{n} \;\&\; \max_a \langle X_a, \mathrm{sgn}(A)\rangle_F^2 \leq \frac{\nu r}{n^2} \qquad (K2)$$

**Poznámky:**

- sgn$(A)$ ... $\lambda_j$ nahradíme sgn$(\lambda_j)$

$$\mathrm{sgn}(A) u_j = \mathrm{sgn}(\lambda_j) u_j$$

- $\|X_a\|_F = 1$, tedy $\|X_a\| \geq \frac{1}{\sqrt{n}}$ ... $\nu \geq 1$ v (K1)
- matice v $T$ mají rank $\leq 2r$ ... (K1) $\Rightarrow$ první půl. (K2)

$$\|P_T X_a\|_F^2 = \sup_{Z \in T, \|Z\|_F = 1} \langle X_a, Z\rangle_F^2 \leq \sup_Z \|X_a\|^2 \cdot \|Z\|_*^2$$

$$\leq \sup_Z \|X_a\|^2 \cdot (2r \cdot \|Z\|_F^2) \overset{(K1)}{\leq} \frac{2r \cdot \nu}{n}$$

**Věta:** Nechť $A$ je $n \times n$ matice s koherencí $\nu$ vzhledem k $\{X_a\}_{a=1}^{n^2}$. Nechť $\Omega$ je náhodná podmnožina s $|\Omega| \geq O(n r \nu (1+\beta) \ln^2 n)$. Pak řešení $(P_*)$ je jednoznačné a rovno $Z$ s $\mathbb{P} \geq 1 - n^{-\beta}$.

**Důkaz:** Pro $Z \in \mathbb{R}^{n \times n}$ položme $\Delta = Z - A$. Chceme ukázat, že

$$\|Z\|_* = \|\Delta + A\|_* > \|A\|_* \quad \text{pokud je } \langle X_{\omega_j}, Z\rangle_F = \langle X_{\omega_j}, A\rangle_F$$

pro $j = 1, \dots, |\Omega|$

... tedy $R(Z) = R(A)$ ... $R(\Delta) = 0$

- je-li $R(\Delta) \neq 0$ ... infeasible ... není v $(P_*)$ ... $\Delta = \Delta_T + \Delta_{T^\perp}$; $\Delta_T = P_T \Delta$.

Krok 1.: Redukce na náhodný sampling s opakováním

- úspěch ($P_*$) klesá s tím, jak se zmenšuje počet podmínek

$$\langle X_{\omega_j}, Z \rangle_F = \langle X_{\omega_j}, A \rangle_F$$

... vyšší počet podmínek zmenšuje ker($R$)... zmenšuje počet feasible $\Delta$ & roste pravd., že $A$ je opravdu prvek s nejm. $\|\cdot\|_*$ v ker($R$) + $A$

Krok 2.: Uvažujme $R = \frac{n}{m^2} \sum_{j=1}^{m} P_{\omega_j}$, $\omega_j$ samplovány nezávisle.

- $\mathbb{E} R = Id$

- $\mathbb{E}[P_T R P_T] = P_T [\mathbb{E} R] P_T = P_T$

- označme $p_1 := \mathbb{P}(\|P_T - P_T R P_T\| \geq 1/2)$

- Nechť $\|P_T - P_T R P_T\| \leq 1/2$ & $\|\Delta_T\|_F^2 \geq 2 m n^2 \|\Delta_{T^\perp}\|_F^2$

Pak $\|R(\Delta_{T^\perp})\|_F^2 \leq \|R\|^2 \cdot \|\Delta_{T^\perp}\|_F^2$

operátorová norma $R: (\mathbb{R}^{n\times n}, \|\cdot\|_F) \to (\mathbb{R}^{n \times n}, \|\cdot\|_F)$ ... $= \frac{n^2}{m} \cdot$ nejvyšší počet kolizí $\leq n^2$

$$\leq n^4 \cdot \|\Delta_{T^\perp}\|_F^2 \leq \frac{n^4}{2mn^2} \cdot \|\Delta_T\|_F^2 \overset{?}{\leq} \frac{n^2}{m} \cdot \underbrace{(1 - \|P_T - P_T R P_T\|)}_{\geq 1/2} \cdot \|\Delta_T\|_F^2$$

$$\leq \frac{n^2}{m} \left( \langle \Delta_T, \Delta_T \rangle_F - \langle [P_T - P_T R P_T] \Delta_T, \Delta_T \rangle \right.$$

$$= \frac{n^2}{m} \left( \langle \Delta_T, \Delta_T \rangle_F - \langle P_T \Delta_T, \Delta_T \rangle_F + \langle P_T R P_T \Delta_T, \Delta_T \rangle_F \right.$$

$$= \frac{n^2}{m} \langle \Delta_T, P_T R P_T \Delta_T \rangle_F = \frac{n^2}{m} \langle \Delta_T, R \Delta_T \rangle_F$$

$$= \frac{n^2}{m} \left\langle \Delta_T, \frac{n^2}{m} \sum_{j=1}^{m}{}' P_{\omega_j}(\Delta_T) \right\rangle = \frac{n^4}{m^2} \sum_{j=1}^{m}{}' \langle \Delta_T, P_{\omega_j}(\Delta_T) \rangle$$

$$= \frac{n^4}{m^2} \sum_{j=1}^{m}{}' \left\langle P_{\omega_j}(\Delta_T), P_{\omega_j}(\Delta_T) \right\rangle = \frac{n^4}{m^2} \sum_{j,k=1}^{m}{}' \langle P_{\omega_j}(\Delta_T); P_{\omega_k}(\Delta_T) \rangle$$

$$= \langle R\Delta_T, R\Delta_T \rangle = \| R \Delta_T \|^2$$

... tedy $\| R(\Delta_{T^\perp}) \|_F^2 < \| R(\Delta_T) \|_F^2$ & $R(\Delta) \neq 0$ ... $\Delta$ je infeasible.

"Zbývá" odhadnout $p_1 := \mathbb{P}(\| P_T - P_T R P_T \| \geq t)$ ... $\leq 4nr \exp\left( \frac{-t^2 m}{4(2n\nu r + 1)} \right)$

pro $t = \frac{1}{2}$ $\qquad\qquad$ $0 < t < 2$

Z Bernsteinovy nerovnosti:

$$S_{\omega_j} = \frac{n^2}{m} P_T P_{\omega_j} P_T - \frac{1}{m} P_T$$

- $$\mathbb{E} S_{\omega_j} = \frac{n^2}{m} P_T [\mathbb{E} P_{\omega_j}] P_T - \frac{1}{m} P_T = \frac{n^2}{m} P_T \Big[ \underbrace{\frac{1}{n^2} \sum_{a=1}^{n^2}{}' P_{a}}_{Id} \Big] P_T - \frac{1}{m} P_T = 0$$

- $$\sum_{j=1}^{m}{}' S_{\omega_j} = \frac{n^2}{m} P_T \left[ \sum{}' P_{\omega_j} \right] P_T - P_T = P_T R P_T - P_T$$

• Odhad $\|S_{\omega_j}\|$

$$\|S_{\omega_j}\| = \left\|\frac{n^2}{m} P_T P_{\omega_j} P_T - \frac{1}{m} P_T\right\| \le \frac{n^2}{m} \underbrace{\|P_T P_{\omega_j} P_T\|} + \frac{1}{m} \underbrace{\|P_T\|}_{\le 1}$$

$$\|P_T P_{\omega_j} P_T(Z)\|_F = \left\|P_T\left(\langle P_T(Z), X_{\omega_j}\rangle_F \cdot X_{\omega_j}\right)\right\|_F$$

$$= |\langle P_T(Z), X_{\omega_j}\rangle_F| \cdot \|P_T(X_{\omega_j})\|_F = |\langle Z, P_T(X_{\omega_j})\rangle| \cdot \|P_T(X_{\omega_j})\|_F$$

$$\le \|Z\|_F \cdot \underbrace{\|P_T(X_{\omega_j})\|_F^2}_{\le \frac{2\nu r}{n}}$$

$$\le \frac{n^2}{m} \cdot \frac{2\nu r}{n} + \frac{1}{m} = \frac{2\nu r n + 1}{m} =: c$$

• $V_0^2$: $\|E[S_{\omega_j}]^2\| = \left\|E\left[\left(\frac{n^2}{m} P_T P_{\omega_j} P_T - \frac{1}{m} P_T\right)^2\right]\right\|$

$$= \left\|E\left(\frac{n^2}{m} P_T P_{\omega_j} P_T\right)^2 - \underbrace{\frac{2n^2}{m^2} E[P_T P_{\omega_j} P_T]}_{-\frac{2n^2}{m^2} \cdot \frac{1}{n^2} Id \cdot P_T} + \frac{1}{m^2} P_T\right\| \qquad E P_{\omega_j} = \frac{1}{n^2} Id$$

$$= \left\|E\left(\frac{n^2}{m} P_T P_{\omega_j} P_T\right)^2 - \frac{1}{m^2} P_T\right\|$$

$$\le \frac{n^4}{m^2} \|E[P_T P_{\omega_j} P_T P_{\omega_j} P_T]\| + \frac{1}{m^2}.$$

$$P_{\omega_j} P_T(Z) \in \operatorname{span}\{X_{\omega_j}\} \quad \text{a} \quad P_{\omega_j} P_T(X_{\omega_j}) = \langle P_T X_{\omega_j}, X_{\omega_j} \rangle X_{\omega_j}$$

... na $\operatorname{span}\{X_{\omega_j}\}$ je $P_{\omega_j} P_T$ totéž jako id. $\langle P_T X_{\omega_j}, X_{\omega_j} \rangle$

$$\Rightarrow P_T P_{\omega_j} P_T (P_{\omega_j} P_T) = P_T \{ \langle P_T X_{\omega_j}, X_{\omega_j} \rangle P_{\omega_j} P_T \}$$

$$\Rightarrow \| \mathbb{E} [ P_T P_{\omega_j} P_T P_{\omega_j} P_T ] \| = \| \mathbb{E} [ \langle P_T X_{\omega_j}, X_{\omega_j} \rangle P_T P_{\omega_j} P_T ] \|$$

$$\leq \underbrace{\max_{\omega} \langle P_T X_{\omega}, P_T X_{\omega} \rangle}_{\leq \frac{2\nu r}{n}} \cdot \underbrace{\| \mathbb{E} [ P_T P_{\omega} P_T ] \|}_{\frac{1}{n^2} \| P_T \|} \qquad \boxed{P_T P_\omega P_T \text{ je samoadj.}}$$

Celkem $\| \mathbb{E} [ S_{\omega_j} ]^2 \| \leq \frac{n^4}{m^2} \cdot \frac{2\nu r}{n} \cdot \frac{1}{n^2} \| P_T \| + \frac{1}{m^2} = \frac{2\nu r n + 1}{m^2} =: V_0^2$

Pro $0 < t < \frac{2mV_0^2}{c} = \frac{2m \cdot \frac{2\nu r n + 1}{m^2}}{\frac{2\nu r n + 1}{m}} = 2$ je

$$2n \exp\left(-\frac{t^2}{4mV_0^2}\right)$$

$$\mathbb{P}(\| P_T - P_T R P_T \| > t) \leq 2 \cdot N \cdot \exp\left(-\frac{t^2 m^2}{4m(2\nu r n + 1)}\right)$$

$$= 2N \exp\left(-\frac{1 \cdot m}{16(2\nu r n + 1)}\right) \quad \text{pro } t = 1/2$$

... operátory uvažujeme def. pouze na $T$

$N = \dim T = 2nr - r^2 \leq 2nr$

$$\ldots \; p_1 \leq 4nr \exp\left(-\frac{m}{16(2\nu r m + 1)}\right)$$

Krok 3: $\Delta_T$ malé ... $\|\Delta_T\|_F^2 < 2un^2 \|\Delta_{T^\perp}\|_F^2$

... bude stačit $\|\Delta_T\|_F^2 < n^4 \|\Delta_{T^\perp}\|_F^2$

& $R(\Delta) = 0$ ... tedy $\Delta \in \ker(R)$ ... $\Delta \in \mathrm{range}(R)^\perp$

Ukážeme, že pak $\|Z\|_* = \|A+\Delta\|_* > \|A\|_*$

• $U := \mathrm{range}(A)$

$$\text{Odhadneme } \|A+\Delta\|_* \overset{\text{pinching ineq.}}{\geq} \|P_U(A+\Delta)P_U\|_* + \|P_{U^\perp}(A+\Delta)P_{U^\perp}\|_*$$

$$= \|\underbrace{P_U A P_U}_{=A} + P_U \Delta P_U\|_* + \|\underbrace{P_{U^\perp} A P_{U^\perp}}_{=0} + P_{U^\perp}(\Delta_T + \Delta_{T^\perp})P_{U^\perp}\|_*$$

$$= \|A + P_U \Delta P_U\|_* + \|\Delta_{T^\perp}\|_* \qquad \Delta_{T^\perp} = P_{T^\perp}\Delta = P_{U^\perp}\Delta P_{U^\perp}$$

$$\geq \langle \mathrm{sgn}(A), A + P_U \Delta P_U \rangle_F + \langle \mathrm{sgn}(\Delta_{T^\perp}), \Delta_{T^\perp} \rangle_F$$

$$= \|A\|_* + \langle \mathrm{sgn}(A), P_U \Delta P_U \rangle_F + \langle \mathrm{sgn}(\Delta_{T^\perp}), \Delta_{T^\perp} \rangle_F$$

$$= \|A\|_* + \langle \mathrm{sgn}(A), \Delta \rangle_F + \langle \mathrm{sgn}(\Delta_{T^\perp}), \Delta \rangle_F$$

A v bázi $\{u_1, \dots, u_n\}$ ... $\left(\begin{array}{c|c} P_U A P_U & P_U A P_{U^\perp} \\ \hline P_{U^\perp} A P_U & P_{U^\perp} A P_{U^\perp} \end{array}\right) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & 0 \end{array}\right)$

pro $\Delta_{T^\perp}$: $\left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & \Delta_{T^\perp} \end{array}\right)$

Ukážeme, že $\langle \mathrm{sgn}(A) + \mathrm{sgn}(\Delta_{T^\perp}), \Delta \rangle_F > 0$ a jsme hotovi!

Ukážeme, že $\exists Y \in \mathrm{range}(\mathcal{R})$ s

$$\|P_T Y - \mathrm{sgn}(A)\|_F \leq \frac{1}{2n^2} \quad \text{a} \quad \|P_{T^\perp} Y\| \leq \frac{1}{2}$$

... pak $Y \in \ker(\mathcal{R})^\perp$ & $\langle Y, \Delta \rangle_F = 0$

$$\Rightarrow \langle \mathrm{sgn}(A) + \mathrm{sgn}(\Delta_{T^\perp}), \Delta \rangle_F$$

$$= \langle \mathrm{sgn}(A) + \mathrm{sgn}(\Delta_{T^\perp}) - Y, \Delta \rangle_F$$

$$= \langle \mathrm{sgn}(A) - Y, \Delta_T \rangle + \langle \mathrm{sgn}(\Delta_{T^\perp}) - Y, \Delta_{T^\perp} \rangle_F$$

$$= \underbrace{\langle \mathrm{sgn}(\Delta_{T^\perp}), \Delta_{T^\perp} \rangle_F}_{= \|\Delta_{T^\perp}\|_*} - \underbrace{\langle P_{T^\perp} Y, \Delta_{T^\perp} \rangle_F}_{\leq \frac{1}{2}\|\Delta_{T^\perp}\|_*} - \underbrace{\langle P_T Y - \mathrm{sgn}(A), \Delta_T \rangle}_{\leq \frac{1}{2n^2}\|\Delta_T\|_F}$$

$$\geq \frac{1}{2}\|\Delta_{T^\perp}\|_* - \frac{1}{2n^2}\|\Delta_T\|_F \geq \frac{1}{2}\|\Delta_{T^\perp}\|_F - \frac{1}{2n^2}\|\Delta_T\|_F > 0.$$

Zbývá: • pinching ineq.
• existence Y

Pinching ineq: $\| P_U Z P_U \|_* + \| P_{U^\perp} Z P_{U^\perp} \|_*$

$$= \sup_{\|A\| \leq 1} \langle P_U Z P_U, A \rangle_F + \sup_{\|B\| \leq 1} \langle P_{U^\perp} Z P_{U^\perp}, B \rangle$$

$$= \sup_{\|A\| \leq 1} \langle Z, P_U A P_U \rangle + \sup_{\|B\| \leq 1} \langle Z, P_{U^\perp} B P_{U^\perp} \rangle$$

$$= \sup_{\|A\| \leq 1, \|B\| \leq 1} \langle Z, P_U A P_U^* + P_{U^\perp} B P_{U^\perp} \rangle$$

$$\leq \sup_{\|C\| \leq 1} \langle Z, C \rangle_F = \|Z\|_* .$$

Existence Y ... za podmínky (K1) -- jinak v původním článku

- $Y \in \mathrm{Range}(R)$
- $\|P_T Y - \mathrm{sgn}(A)\|_F \leq \frac{1}{2n^2}$
- $\|P_{T^\perp} Y\| \leq \frac{1}{2}$

$P_T Y$ má být blízko $\mathrm{sgn}(A)$ ... logická volba by byla

$$Y := \frac{n^2}{m} \sum_{i=1}^{m} \langle X_{\omega_i}, \mathrm{sgn}(A) \rangle_F \cdot X_{\omega_i} = R(\mathrm{sgn}(A))$$

... konvergují pomalu $\Rightarrow$ Golfing scheme

Položme $Y_1 := \frac{n^2}{k} \sum_{i=1}^{k} \langle X_{\omega_i}, \mathrm{sgn}(A) \rangle X_{\omega_i}$

$$Y_2 := Y_1 + \frac{n^2}{k} \sum_{i=k+1}^{2k} \langle X_{\omega_i}, \mathrm{sgn}(A) - P_T Y_1 \rangle_F X_{\omega_i}$$

$\vdots$

... konvergují exp. rychle v $l = m/k$

Lemma: Pro $Z \in T$ platí

$$\mathbb{P}(\|P_{T^\perp} R(Z)\| > t) \leq \begin{cases} 2n \exp\left(-\frac{t^2 m}{4\nu n \|Z\|_F^2}\right), & t \leq \sqrt{2/r} \cdot \|Z\|_F \\ 2n \exp\left(-\frac{t m}{2\nu \sqrt{2r}\, n \|Z\|_F}\right), & t > \sqrt{2r}\, \|Z\|_F \end{cases}$$

Rozdělme $m = m_1 + \dots + m_\ell$ a definujme

$$R_i : Z \to \frac{n^2}{m_i} \sum_{j = m_1 + \dots + m_{i-1} + 1}^{m_1 + \dots + m_i} \langle X_{\omega_j}, Z \rangle_F X_{\omega_j}$$

$$Y_0 := 0 \ ; \ Z_0 = sgn(A)$$

$$Y_i := Y_{i-1} + R_i(Z_{i-1}) = \sum_{j=1}^{i} R_j(Z_{j-1})$$

$$Z_i = sgn(A) - P_T Y_i$$

$Y_i$ ... i-tá iterace

$Z_i$ ... chyba i-té iterace

Pak $Z_0 := sgn(A)$

$$Z_1 = sgn(A) - P_T Y_1 = sgn(A) - P_T R_1 sgn(A) = (Id - P_T R_1 P_T) sgn(A)$$

$$Z_2 = sgn(A) - P_T(Y_2) = sgn(A) - P_T(Y_1 + R_2 Z_1) =$$

$$= sgn(A) - P_T(R_1 P_T sgn(A) + R_2(Id - P_T R_1 P_T) sgn(A))$$

$$= (Id - P_T R_1 P_T) sgn(A) - P_T R_2 (Id - P_T R_1 P_T) sgn(A)$$

$$= (Id - P_T R_2 P_T)(Id - P_T R_1 P_T) sgn(A)$$

⋮

obecně $Z_i = (Id - P_T R_i P_T) \dots (Id - P_T R_1 P_T) sgn(A)$

... s $\mathbb{P} = p_2(i)$ nechť ~~ne~~platí $\| Id - P_T R_i P_T \| \leq 1/2$ ... prob. of failure

$$\| Z_i \|_F = \| (\cancel{Id}^{\,P_T} - P_T R_i P_T) Z_{i-1} \|_F \leq \frac{1}{2} \| Z_{i-1} \|_F$$

$$\| Z_0 \|_F = \sqrt{r}$$

... pak $\| Z_i \|_F \leq \frac{\sqrt{r}}{2^i}$

- s prav. of failure $p_3(i)$

$$\|P_{T^\perp} R_i Z_{i-1}\| \le \frac{1}{4\sqrt{r}} \|Z_{i-1}\|_F$$

$$\Downarrow \|P_{T^\perp} Y_\ell\| = \|P_{T^\perp}(\sum_{j=1}^{\ell} R_j Z_{j-1})\| \le \sum_{j=1}^{\ell} \|P_{T^\perp} R_j Z_{j-1}\| \le \frac{1}{4\sqrt{r}} \sum_{j=1}^{\ell} \|Z_{j-1}\|_F$$

$$\le \frac{1}{4\sqrt{r}} \sum_{j=1}^{\ell} \frac{\sqrt{r}}{2^{j-1}} \le \frac{1}{4} \cdot \left(\frac{1}{2} + \frac{1}{4} + \dots\right) = \frac{1}{2}.$$

a $\|Z_\ell\| = \|P_T Y_\ell - \mathrm{sgn}(A)\| \le \frac{\sqrt{r}}{2^\ell} \le \frac{1}{2n^2}$ pro $\ell = \lceil \log_2(2n^2\sqrt{r}) \rceil$

... vlastnosti (ii) & (iii)

pro dual certificate $Y$ ... (i) je jasná!

---

Zbývá Lemma & důkaz, že $p_1 + \sum_{i=1}^{\ell} p_2(i) + \sum_{i=1}^{\ell} p_3(i) \le n^{-\beta}$.

- $p_1 = 4nr \exp\left(-\frac{m}{16(2\nu rn+1)}\right)$

- $p_2$: $\mathbb{P}\left(\|P_T - P_T R_i P_T\| \ge \frac{1}{2}\right) \le 4nr \exp\left(-\frac{m_i}{16(2\nu rn+1)}\right) = p_2(i)$

- $p_3$ ... Lemma: $\mathbb{P}\left(\|P_{T^\perp} R Z_{i-1}\| > \frac{\|Z_i\|_F}{4\sqrt{r}}\right) \le 2n \exp\left(-\frac{\overbrace{\|Z_i\|_F^2 / 16r}^{t^2} \cdot m_i}{4\nu n \cdot \|Z_{i-1}\|_F^2}\right)$

$$= 2n \exp\left(-\frac{m_i}{64\nu n r}\right)$$

Choose $p_1 \le \frac{n^{-\beta}}{3}$ ; $p_2(i) \le \frac{n^{-\beta}}{3l}$ ; $p_3(i) \le \frac{n^{-\beta}}{3l}$

2: $l \cdot 4nr \exp\left(-\frac{m_i}{16(2\nu r m+1)}\right) \le n^{-\beta}/3$

$12 l n^{(1+\beta)} r \le \exp\left(\frac{m_i}{16(2\nu r m+1)}\right) \ldots \ln(12 l n^{(1+\beta)} r) \le \frac{m_i}{16(2\nu r m+1)}$

$m_i \ge 16(2\nu r m+1) \ln(12 l n^{(1+\beta)} r)$

3: $2n \exp\left(-\frac{m_i}{64\nu m r}\right) \le \frac{n^{-\beta}}{3l} \ldots \ln(6 l n^{1+\beta}) \le \frac{m_i}{64\nu m r}$

$m_i \ge 64\nu m r \ln(6 l n^{1+\beta})$

recall: $l \simeq \log_2(2n^2\sqrt{r}$
$\simeq \log(n)$

$\Rightarrow m \ge 64\nu m r l \cdot \ln(12 l n^{1+\beta} \cdot r)$

$= O(\nu r n \cdot \log n \cdot (1+\beta) \log n)$ •