

Beier, Vocking: Random Knapsack in Expected Polynomial Time

brute-force + dominancia

$S \subseteq \{1, \dots, n\}$, váha $W(S)$, profit $P(S)$

dominuje $T \subseteq \{1, \dots, n\}$ ak $W(S) \leq W(T) \wedge P(S) \geq P(T)$

- $S(i)$ postupnosť dominujúcich množín nad $\{1, \dots, i\}$
- $S(i) \longrightarrow S(i + 1)$ //merge
- $f_i(t)$ max. profit s váhou t pri $\{1, \dots, i\}$

lema $\forall i \in \{1, \dots, n\}$ $q(i)$ je horný odhad na počet dominujúcich nad $\{1, \dots, i\}$, $q(i + 1) \geq q(i)$. Potom algoritmus počíta v očakávanom čase

$$O\left(\sum q(i)\right) = O(n \cdot q(n))$$

rovnomé rozdelenie profitov z $(0, 1)$, váhy určuje adversary

Thm: $E[q] = O(n^3)$

// RAM s jednotkovou cenou, $\{+, -, *, DIV_2, \log_2, EXP_2\}$

- $m = 2^n, S_1, \dots, S_m$
- $P_u = \sum_{i \in S_u} p_i$
- $\Delta_u = \max_{\nu \in \{1, \dots, u\}} P_\nu - \max_{\nu \in \{1, \dots, u-1\}} P_\nu$
ak $\Delta_u > 0$ tak S_u je dominujúca

lema $\forall u \in \{2, \dots, m\} \quad E[\Delta_u | \Delta_u > 0] \geq \frac{1}{32n^2}$

potom:

- $P_m = \sum_{1 \leq i \leq m} p_i, P_1 = \sum_{i \in S_1} p_i = 0$
- $E[P_m] = P_1 + \sum_{u=2}^m E[\Delta_u] = \sum_{u=2}^m Pr[\Delta_u > 0] E[\Delta_u | \Delta_u > 0] \geq \sum_{u=2}^m Pr[\Delta_u > 0] \frac{1}{32n^2}$
- $E[P_m] = n/2$
- $E[q] = 1 + \sum_{u=2}^m Pr[\Delta_u > 0] \leq 1 + 32n^2 E[P_m] \leq 16n^3 + 1$

$$\forall u \in \{2, \dots, m\} \quad E[\Delta_u \mid \Delta_u > 0] \geq \frac{1}{32n^2}$$

dôkaz lemy

fix u

- keďže $E[\Delta_u \mid \Delta_u > 0] \geq Pr[\Delta_u \geq \frac{1}{16n^2} \mid \Delta_u] \cdot \frac{1}{16n^2}$,
stačí argumentovať $Pr[\Delta_u \geq \frac{1}{16n^2} \mid \Delta_u > 0] \geq 1/2$

- $X_v = S_u \setminus S_v, Y_v = S_v \setminus S_u$

- $Pr[\Delta_u \geq \frac{1}{16n^2} \mid \Delta_u > 0]$
 $= Pr[\forall v \sum_{i \in S_u} p_i \geq \sum_{i \in S_v} p_i + \frac{1}{16n^2} \mid \forall v \sum_{i \in S_u} p_i > \sum_{i \in S_v} p_i]$
 $= Pr[\forall v \sum_{i \in X_v} p_i \geq \sum_{i \in Y_v} p_i + \frac{1}{16n^2} \mid \forall v \sum_{i \in X_v} p_i \geq \sum_{i \in Y_v} p_v]$

- w.l.o.g. $S = \{1, \dots, k\}$
- náhodné premenné $\underbrace{\{p_1, \dots, p_k\}}_I, \underbrace{\{p_{k+1}, \dots, p_n\}}_{II}$
- $X_v \rightsquigarrow I, X_u \rightsquigarrow II; \quad \text{fix } \{p_{k+1}, \dots, p_n\}$
- $Pr[\exists j \in \{1, \dots, k\} : p_j \leq \frac{1}{4n} \mid \forall v \sum_{i \in X_v} p_i \geq \sum_{i \in Y_v} p_i]$
 $\leq \sum_{j \in \{1, \dots, k\}} Pr[p_j \leq \frac{1}{4n} \mid \forall v \sum_{i \in X_v} p_i \geq \sum_{i \in Y_v} p_i]$
 $\leq \sum_{j \in \{1, \dots, k\}} Pr[p_j \leq \frac{1}{4n}] = \frac{k}{4n} \leq 1/4$
- predpokladáme, že $p_j > 1/4n \quad \forall j \in \{1, \dots, k\}$
- $L_v = \sum_{i \in X_v} p_i, L_v \geq \frac{1}{4n}$
- chceme $Pr[\Delta_u \geq \frac{1}{16n^2} \mid \Delta_u > 0]$
 $= Pr[\forall v \sum_{i \in S_u} p_i \geq \sum_{i \in S_v} p_i + \frac{1}{16n^2} \mid \forall v \sum_{i \in S_u} p_i > \sum_{i \in S_v} p_i]$
 $= Pr[\forall v \sum_{i \in Y_v} p_i \leq L_v - \frac{1}{16n^2} \mid \forall v \sum_{i \in Y_v} p_i \leq L_v] \geq 3/4$

$$\mathcal{A} = \{(p_{k+1} \times \cdots \times p_n) \in (0, 1)^{n-k} \mid \forall v \sum_{i \in Y_v} p_i \leq L_v - \frac{1}{16n^2}\}$$

$$\mathcal{B} = \{(p_{k+1} \times \cdots \times p_n) \in (0, 1)^{n-k} \mid \forall v \sum_{i \in Y_v} p_i \leq L_v\}$$

$$\mathcal{A} \subseteq \mathcal{B}$$

$$Pr[\Delta_u \geq \frac{1}{16n^2} \mid \Delta_u > 0] = \frac{vol(\mathcal{A} \cap \mathcal{B})}{vol(\mathcal{B})} = \frac{vol(\mathcal{A})}{vol(\mathcal{B})} \quad \text{chceme} \geq 3/4$$

$$\forall \epsilon \in (0, 1) \mathcal{B}_\epsilon = \{(p_{k+1} \times \cdots \times p_n) \in (0, 1 - \epsilon)^{n-k} \mid \forall v \sum_{i \in Y_v} p_i \leq (1 - \epsilon)L_v\}$$

$$\mathcal{B}_\epsilon = \mathcal{B}, \quad vol(\mathcal{B}_\epsilon) = (1 - \epsilon)^{n-k} vol(\mathcal{B})$$

$$\text{chceme } \epsilon : \mathcal{B}_\epsilon \subseteq \mathcal{A}$$

$$L_v(1 - \frac{1}{4n}) \leq L_v - \frac{1}{16n^2} \quad \text{predp. } L_v \geq 1/4n$$

$$\epsilon = \frac{1}{4n} \rightsquigarrow vol(\mathcal{A}) \geq vol(\mathcal{B}_\epsilon) = (1 - \epsilon)^{n-k} vol(\mathcal{B}) \geq (1 - \epsilon(n - k)) vol(\mathcal{B}) \geq \frac{3}{4} vol(\mathcal{B})$$

□ lema

Noam Livne: All Natural NPC Problems Have Average-Case Complete Versions

distributional problem — rozhodovací problém + pravdepodobnostné rozdelenie
chceme dobrý očakávaný čas alebo PTIME a nízka pravdepodobnosť chyby

kvalita výsledkov o obtiažnosti priemernej zložitosti

- 1 rozsah platnosti
- 2 prirodzenosť rozhodovacieho problému
- 3 jednoduchosť pravdepodobnostného rozdelenia
- 4 rôznorodosť získaných ťažkých problémov

Ako ukážeme, že NP rozhodovací je v priemere ťažký?

- je ťažký pre triedu pravdepodobnostných rozdelení
 - čo najširšia trieda rozdelení
 - čo najpopulárnejší problém
 - čo najbližšie k rovnomernému rozdeleniu

Levin

namiesto rovnomerného P-computable rozdelenie: akumulatívna pravdepodobnosť vypočítateľná v PTIME ($\tilde{\mu}(x) = \sum_{x' < x} \mu(x')$)

- avgP distributional problémy efektívne riešiteľné v priemere
- distNP NP pri P-computable rozdeleniach
- AP-redukcie zachovávajú jednoduchosť v priemere (redukcia nemôže príliš meniť pravdepodobnostné rozdelenie)

- existuje dist-NP úplný
- $distNPC \in avgP \Leftrightarrow distNP \subseteq avgP$

príspevok tohto článku - jednoduchá postačujúca podmienka aby NPC A mal rozdelenie μ pri ktorom (A, μ) je distNPC

postup:

- 1 konštrukcia monotónnej Karp redukcie (transformácia ľubovoľnej na monotónu)
- 2 ak existuje monotónna redukcia (rozhodovacej časti) nejakého distNPC A na NPC B , tak pre NPC B existuje rozdelenie μ , že (B, μ) je distNPC

neformálne

- $(C, \mu) \in \text{distNPC}$
- redukcia $C \xrightarrow{h} SAT : |x| \geq |y| \Leftrightarrow |h(x)| \geq |h(y)|$
- Karp-redukcia f , pričom $w \xrightarrow{f} h(w)$
 $f(w) = e_{w_1} \wedge e_{w_2} \wedge \dots \wedge e_{w_{|w|}} \wedge h(w)$ $e_0 = (x_0 \vee \neg x_0), e_1 = (x_1 \vee \neg x_1)$
monotónnosť: $w \prec w' \Rightarrow f(w) \prec f(w')$
P-invertibility: $f^{-1}(w) \in \text{PTIME}$
zachovanie splniteľnosti

Pre rozdelenie

$$\eta(x) = \begin{cases} \mu(f^{-1}(x)), & x \in \text{Im}(f) \\ 0, & \text{inak} \end{cases}$$

je f APredukcia (C, μ) na SAT, η

1-1 f je P-invertovateľná ak existuje PTIME A : $A(x) = \begin{cases} f^{-1}(x), & \text{ak existuje} \\ \perp, & \text{inak} \end{cases}$

f je length-regular ak $\forall x, y \in \{0, 1\}^* : |x| \leq |y| \Leftrightarrow |f(x)| \leq |f(y)|$

f je semi-monotónna ak $\forall x, y \in \{0, 1\}^*, |x| = |y| \mid |x| < |y| \Leftrightarrow |f(x)| < |f(y)|$

AP-redukcia (S, μ_S) do (T, μ_T) : many-one PTIME redukcia z S do T plus polynóm q taký, že $\forall y \in \{0, 1\}^* : \mu_T(y) \geq \frac{1}{q(|y|)} \sum_{x \in f^{-1}(y)} \mu_S(x)$

pre 1-1 redukciiu f $\mu_T(f(x)) \geq \frac{\mu_S(x)}{q(|x|)}$

$$\text{avgP} = \left\{ (L, \mu) \mid \exists A : L = L(A), \exists \lambda > 0 \quad \sum_{x \in \{0,1\}^*} \mu(x) \frac{t_A(x)^\lambda}{|x|} < \infty \right\}$$

technika—nafukovanie(padding)

L je regulárne nafúknuteľný ak \exists rastúca fcia q a padding fcia $S : 1^* \times \Sigma^* \rightarrow \Sigma^*$

- S je PTIME
- zachováva príslušnosť: $S(1^n, x) \in L \Rightarrow x \in L$
- regulárna dĺžka: $\forall n, x : n > |x|$ platí, že $|S(1^n, x)| = q(n)$

lema Ak je rozhodovací problém regulárne-nafúknuteľný tak každú Karp redukciiu naň možno prerobiť na length-regular

—vezmemem rastúci polynóm $r : r(|x|) \geq |f(x)|$ a definujeme

$$f'(x) = S(1^{r(|x|)}, f(x))$$

L je monotónne nafúknuteľný ak existuje padding fcia $E : \Sigma^* \times \Sigma^* \longrightarrow \Sigma^*$

- E je PTIME
- zachováva príslušnosť: $E(p, x) \in L \iff x \in L$
- semimonotónnosť: $p < p', |p| = |p'|, |x| = |x'|$ potom $E(p, x) < E(p', x')$
- length-regularita: $|x| = |x'|, |p| = |p'|$ potom $E(p, x) = E(p', x')$ a ak $|x| < |x'|$ a $|p| \leq |p'|$ tak $E(p, x) < E(p', x')$

fakt Ak $E(p, x) = e_{p_1}e_{p_2} \dots e_{p_{|p|}}g(x)$, pričom

- $|e_0| = |e_1|$ a $e_0 < e_1$
- $g(x)$ je length-regular
- $E(p, x) \in L \iff x \in L$

tak E je monotónne nafúknuteľná pre L

Ak L je NPC, regulárne nafúknuteľný a monotónne nafúknuteľný, potom existuje distribúcia η taká, že (L, η) je distNPC.

Dôkaz redukciami z distNPC (C, μ)

// Levin–existuje

$C \xrightarrow{h} L$, E regular padding, D monotone-padding

• h transformujeme na regulárnu dĺžku zachovávajúcu h' , $C \xrightarrow{h'} L$ lema

• def $f(x) = E(x, h'(x))$

– f je príslušnosť zachovávajúca redukcia C do L

– f zachováva regulárnu dĺžku (lebo h' , E sú také)

– f je semimonotónna (lebo h' je length-regular, E je seimonotónna)

f je monotónna, $f^{-1}(y) \leq f(y)$

$$y \xrightarrow{\text{binarySearch}} \begin{cases} x, & x = f^{-1}(y) \\ \perp, & f(x) < y < f(x + 1) \end{cases}$$

preto je f P-invertovateľná

$$\eta(x) = \begin{cases} \mu(f^{-1}(x)), & x \in \text{Im}(f) \\ 0, & \text{inak} \end{cases}$$

- f zachováva pravdepodobnosť inštancií
- μ je P-computable, f je invertovateľná, $\bar{\eta}(y) = \bar{\mu}(x)$, kde x je najväčšie také, že $f(x) \leq y$, preto je η P-computable

$$\hookrightarrow (C, \mu) \xrightarrow{f} (SAT, \eta)$$

□

SAT má distribučnú verziu, ktorá je *distNPC*

"bezkontextové" kódovanie formúl, aby regular paddable, monotónne paddable

- regular

$$\Phi(x_1, \dots, x_n) \rightsquigarrow e_{w_1} \wedge e_{w_2} \wedge \dots \wedge e_{w_{|\Phi|}} \wedge \Phi(x_{|\Phi|+1}, \dots, x_{|\Phi|+n}) \quad e_0 = (x_0 \vee \neg x_0), \dots$$

- monotónne kódovanie

klika má distribučnú verziu, ktorá je *distNPC*

G maticou, k binárne

$$n^2 + \lceil \log n \rceil$$

- regular

izolované vrcholy $n^2 + \lceil \log n \rceil \rightsquigarrow m^2 + \lceil \log m \rceil$

$$q(n) = n^2 + \lceil \log n \rceil$$

- **monotónne** kódovanie $E(p, (M, k)) = (M', k)$:

rozmer M' je $(n + |p|) \times (n + |p|)$

$$M'(i + |p|, j + |p|) = M(i, j), \quad M'(1, j) = p_j \quad // \quad p_j \text{ je } j\text{-ty bit } p$$

čo s novými klikami dĺžky 2? Ak $k = 2 \wedge G$ nemá hrany, E zmení $k = 2 \rightarrow 3$

□

HK má distribučnú verziu, ktorá je *distNPC*

- regular

n -vrcholový graf \rightsquigarrow $(n + k)$ -vrcholový pri zachovaní existencie HK

$$E' = E \cup \{(v_{n+i}, v_{n+i+1}) \mid 0 \leq i \leq k - 1\} \cup \{(u, v_{n+k}) \mid (u, v_n) \in E\}$$

- **monotónne** kódovanie $E(p, M) = (M')$:

rozmer M' je $(n + |p| + 2) \times (n + |p| + 2)$

$$M'(i + |p| + 2, j + |p| + 2) = M(i, j)$$

$$M'(1, i + |p| + 2) = M(1, i)$$

$$M'(i, i + 1) = 1, \quad 1 \leq i \leq |p| + 2$$

$$M'(1, i + 2) = p_i, \quad 1 \leq i \leq |p| + 2$$

//cesta na začiatku

//kódovanie p

□