Aproximační metoda:

- většinou se používá na optimalizační úlohy

Obchodní cestující – 2-aproximační:

- nalezneme kostru, kterou obejdeme tam a zpátky, občas můžeme z listu vzít zkratku, každopádně proti opt. Ham. kružnici budeme nejvíce 2x delší.

Věta: Pokud $P \neq NP$ a $\rho \geq 1$, potom neexistuje polyn. aprox. alg. pro problém obch. cest.

Dk: Sporem: Pokud by takový alg. existoval, vyřešili bychom problém ham. kružnice v polyn. čase, přestože je to NPÚ problém.

Nechť $G = (V, E)$ je instancí problému ham. kružnice.

Transformujeme G na instanci POC:

$G' = (V, E')$ je úplný na V, tj: $E' = \{(u,v) \mid u,v \in V \wedge u \neq v\}$

kde cena hrch.

$$c(u,v) \begin{cases} 1 & \text{pokud } (u,v) \in E \\ \rho \cdot |V| + 1 & \text{jinak} \end{cases}$$

– t je polynomiální tvorba

a) Pokud G měl Ham. kružnici, pak v G' je nejlepší cyklus o ceně $|V|$.

b) Pokud G neměl Ham. kružnici, pak každý cyklus v G' obsahuje hranu mimo E a cena cyklu bude alespoň

$$(\rho \cdot |V| + 1) + (|V| - 1) > \rho \cdot |V|$$

Protože hrany v $E' \setminus E$ jsou dlouhé, je velký rozdíl v cyklu $\in E$ a cyklu $\in E'$.

Potom by alg v polyn. čase měl v a) rozhodnout, zda existuje ham. kružnice. Pokud b), vrátí cenu alespoň $\rho \cdot |V|$, tedy jsme polyn. vyřešili problém Ham. kružnice. ↯

$\boxtimes$

Problém batohu:

(S,t), kde $S=\{a_1 \dots a_n\}$, $t \in \mathbb{N}^+$. Rozhodovací problém:

$\exists\, S' \subseteq S$ t.ž. $\sum_{a_i \in S'} a_i = t$

optimalizační: součet max. $a \leq t$.

Značení: $S.+.x = \{s+x, s \in S\}$ pro množinu S i seznam S

Algoritmus: SoučetPodmnožinyPřesně(S,t)

1 $n := |S|$;
2 $L_0 := \langle 0 \rangle$ // seznamy
3 for $i := 1$ to n do
4 $\quad L_i :=$ mergeList($L_{i-1}, L_{i-1}.+.a_i$)
5 $\quad$ vypusť z L_i všechny prvky větší než t
6 return(maximum z L_n)

Procedura mergeList sloučí uspořádané seznamy do uspořádaného seznamu

- délka L_i je až 2^i, tj. alg. je exponenciální (v obecnosti)

Aproximační schéma:

idea: každý seznam L_i po vytvoření "zkrátíme". Používáme parametr $\delta, 0 < \delta < 1$. Zkrátit seznam L znamená vypustit co nejvíc prvků z L tak, že pro každý vypuštěný prvek y zůstal v seznamu L prvek $z \leq y$ takový, že $\frac{y-z}{y} \leq \delta$, tj. $(1-\delta)y \leq z \leq y$.

body zvoleně blízko od sebe

Prvek z je reprezentant y s "dostatečně malou chybou" a musí být, kvůli správnosti, menší než y.

Algoritmus: součetPodmnožinyAprox(S,t, ϵ)

1 $n := |S|$
2 $L_0 := \langle 0 \rangle$
3 for $i := 1$ to n do
4 $\quad L_i :=$ mergeList($L_{i-1}, L_{i-1}.+.a_i$)
5 $\quad L_i :=$ zkrať ($L_i, \epsilon/n$)
6 $\quad$ odstraň z L_i všechny prvky větší než t
7 nech z je největší hodnota v L_n
8 return z

- prvky L_i jsou součty podmnožin
- chceme: $C^*(1-\epsilon) \leq C$ pro cenu C nalezeného a C^* optimální řešení.
- v každém kroku zavádíme chybu ϵ/n, indukcí podle i lze dokázat, že pro každý prvek $y^* \leq t$ z nezkrácené verze existuje $z \in L_i$, tž. $(1-\epsilon/n)^n y^* \leq z \leq y^*$, protože $1-\epsilon \leq (1-\epsilon/n)^n \Rightarrow (1-\epsilon)y^* \leq z$
- navíc, z se nezahodí v kroku 6, protože $z \leq y^* \leq t$
- schéma je úplně polynomiální:

Idea: relativní chyba ϵ/n rozsah $1..t$ rozdělí na polynomiální počet úseků, v každém je ≤ 2 reprezentantů.

Pravděpodobnostní alg: (Test prvočíselnosti) RSA

Las Vegas a Monte Carlo

randomizace pivotu, např.:

občas dělám náhodný krok s nějakou pravděpodobností

Algoritmus: součetPodmnožinyAprox(S,t, ϵ)
1 $n := |S|$
2 $L_0 := \langle 0 \rangle$
3 for $i := 1$ to n do
4 $\quad L_i :=$ mergeList$(L_{i-1}, L_{i-1}. + .a_i)$
5 $\quad L_i :=$ zkrať $(L_i, \epsilon/n)$
6 $\quad$ odstraň z L_i všechny prvky větší než t
7 nech z je největší hodnota v L_n
8 return z

- prvky L_i jsou součty podmnožin
- chceme: $C^*(1-\epsilon) \leq C$ pro cenu C nalezeného a C^* optimální řešení.
- v každém kroku zavádíme chybu ϵ/n, indukcí podle i lze dokázat, že pro každý prvek $y^* \leq t$ z nezkrácené verze existuje $z \in L_i$, tž. $(1-\epsilon/n)^n y^* \leq z \leq y^*$, protože $1-\epsilon \leq (1-\epsilon/n)^n \Rightarrow (1-\epsilon)y^* \leq z$
- navíc, z se nezahodí v kroku 6, protože $z \leq y^* \leq t$
- schéma je úplně polynomiální:
Idea: relativní chyba ϵ/n rozsah $1..t$ rozdělí na polynomiální počet úseků, v každém je ≤ 2 reprezentantů.