460-4005/01: Teoretická informatika (TI)
přednáška 14

prof. RNDr Petr Jančar, CSc.

katedra informatiky FEI VŠB-TUO
www.cs.vsb.cz/jancar

LS 2010/2011

Optimalizační problémy (připomenutí)

Ke každému vstupu množina přípustných řešení,
na nich definována cílová funkce (objective function),
hledaným výstupem je (nějaké) optimální řešení
(tj. s minimální, či maximální, hodnotou cílové funkce).

Příklady:
- minimální kostra v (hranově-ohodnoceném) grafu
- problém obchodního cestujícího

U min. kostry hltavý (greedy) přístup vede k řešícímu polynomiálnímu algoritmu.
Jak je o u TSP ?

Název: TSP (problém obchodního cestujícího) (ANO/NE verze)
Vstup: množina „měst“ $\{1, 2, \ldots, n\}$, přir. čísla („vzdálenosti“) d_{ij} ($i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, n$); dále číslo ℓ („limit“).
Otázka: existuje „okružní jízda“ dlouhá nejvýše ℓ, tj. existuje permutace $\{i_1, i_2, \ldots, i_n\}$ množiny $\{1, 2, \ldots, n\}$
tž. $d(i_1, i_2) + d(i_2, i_3) + \cdots + d(i_{n-1}, i_n) + d(i_n, i_1) \leq \ell$?

Aproximační algoritmy

Jde nám o řešení NP-těžkých optimalizačních problémů (např. TSP).

Potřebujeme polynomiální algoritmus A, který k zadanému vstupu (instanci) I vydá „pokud možno co nejlepší“ přípustné řešení $A(I)$.

Optimální řešení $s_{opt}(I)$ má hodnotu (cílové funkce) $f(s_{opt}(I))$, označme $m(I) = f(s_{opt}(I))$.
Pro algoritmus A označme $m_A(I) = f(A(I))$.

Jde nám o co nejlepší (nejmenší) *aproximační poměr*, v případě minimalizačního problému $\frac{m_A(I)}{m(I)}$.

Např. pro Δ-TSP (tj. TSP, kde v instancích je splněna trojúhelníková nerovnost) existuje 2-aproximační algoritmus, tj. je zaručeno

$$\frac{m_A(I)}{m(I)} \leq 2\,.$$

(Toto je ilustrováno jednou z animací.)

Pravděpodobnostní algoritmy

Přiblížili jsme si elementární základy zachycené v sekci 10.4., ilustrované na problému prvočíselnosti. Uvědomili jsme si, že algoritmus

> *Máš-li testovat prvočíselnost zadaného (např. několikasetmístného) k, projdi všechna $a, 1 < a < k$, a zjišťuj, zda Divides(a, k) (tedy zda $(k \mod a) = 0$) ...*

je exponenciální (ve velikosti zápisu k). (A to i při přímočarých vylepšeních, při nichž zkoumáme jen lichá $a \leq \sqrt{k}$ apod.)
Také jsme si všimli, že pravděpodobnostní algoritmus

> *Vygeneruj náhodné a (řekněme liché $a, 1 < a \leq \sqrt{k}$); jestliže Divides(a, k), return NE, jinak return ANO.*

nám moc nepomůže. (Např. pro velké číslo $m = pq$, kde p, q jsou prvočísla, je náhodná trefa jednoho z dělitelů p, q téměř nemožná.)
Pak jsme naznačili, že (malá) Fermatova věta je základem podstatně lepšího algoritmu, u nějž máme zaručenu minimálně 50% pravděpodobnost nalezení svědka složenosti.

Šifrovací systém s veřejným klíčem; RSA

Uvedení systému jen motivovalo zkoumání problému prvočíselnosti. (Více bude v příštím semestru ve volitelném předmětu Vybrané partie teoretické informatiky.)

1. Zvol dvě náhodná různá (velká, např. 100-místná) prvočísla p, q.
2. Spočítej součiny $n = pq$ a $\Phi(n) = (p-1)(q-1)$.
3. Urči (malé) e tž. $\gcd(e, \Phi(n)) = 1$ (gcd označuje největší společný dělitel).
4. Vypočti d tž. $de \equiv 1 \pmod{\Phi(n)}$.
5. Zveřejni dvojici (e, n); šifrovací funkce je $enc_X(m) = m^e \bmod n$.
6. Drž v tajnosti (d, n); dešifrovací funkce je $dec_X(m) = m^d \bmod n$.