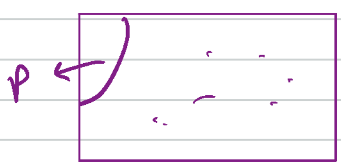
Lecture 24

CS 170

Sanjam Garg.

NP - complete problems still need a solution.

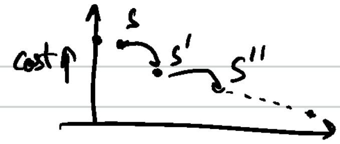


1) "Intelligent" exponential search. → Running time could be exponential
   → Practical instances ↳ run efficiently.

2) Approximation Algorithms. ⟶ polytime
   ↳ relationship with the optimal solution.

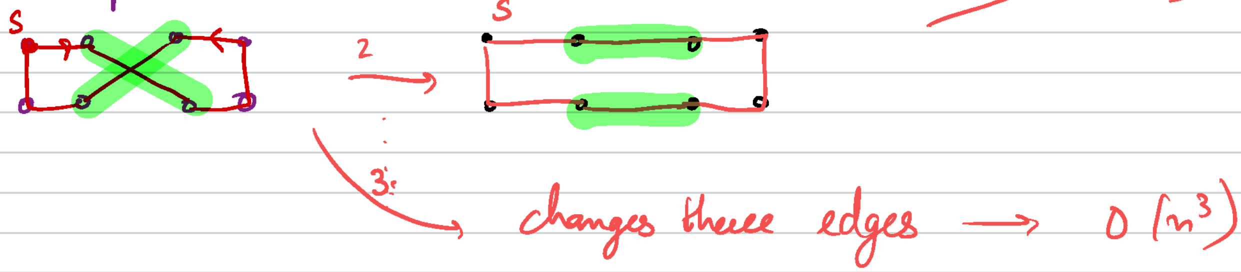
3) Heuristic → no guarantees on the runtime or the optimality of solution.

Local Search Heuristics



> Let s be any initial solution
> while there is some solution s' in the neighborhood of s
> for which $cost(s') < cost(s)$: replace s by s'
> return s

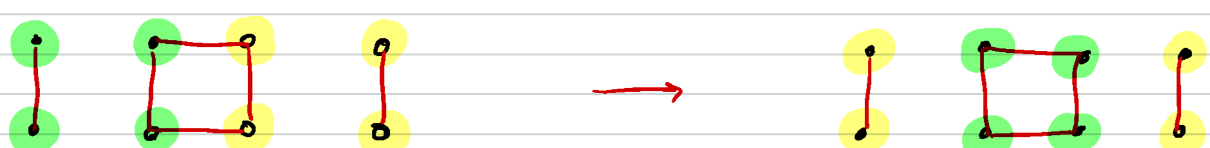
TSP problem

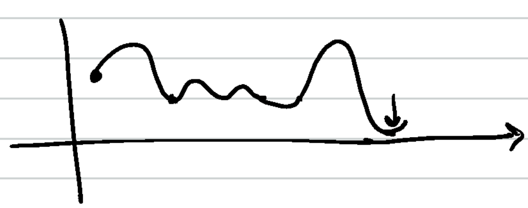


Graph Partitioning

Input: an undirected graph $G = (V, E)$ with non-negative edge weights

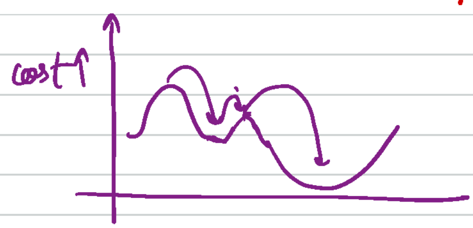
Output: A partition of vertices into groups A & B s.t.
$|A| = |B|$ and minimizing capacity of cut (A, B)





Randomization and restarts

Simulated annealing (introduce temperature parameter T)



Let s be any initial solution

randomly choose a solution s' in the neighborhood of s

if $cost(s') < cost(s)$: replace s by s'

else : replace s by s' with probability $e^{-\frac{(cost(s') - cost(s))}{T}}$

Thinking of NP as a proof. (Interactive Proofs)

ϕ

prover $\leftarrow$ P $\xrightarrow{w \text{ satisfying assignment}}$ V $\rightarrow$ poly time verifier. $\rightarrow$ is $\phi(w)$ 0 or 1?

Completeness: If "ϕ is true" then in $P(\phi, w) \leftrightarrow V(\phi)$ V outputs 1

Soundness: If "ϕ is false" then in $P(\phi, w) \leftrightarrow V(\phi)$ V outputs 1 with very small probability e.g. 2^{-n} (n is some parameter)

$A \times B = C \rightarrow \gg O(n^2)$

$n \times n \leftarrow A, B$, $C = A \times B$

$P \xrightarrow{C} V$ A, B, C $O(n^2)$

① $r \leftarrow \{1 \ldots q\}$ large prime $\vec{r} = (1, r \ldots r^{n-1})$

② $\underbrace{C \times \vec{r}}_{O(n^2)} \stackrel{?}{=} (A \times B) \times \vec{r} = \underbrace{A \times \underbrace{(B \times \vec{r})}_{O(n^2)}}_{O(n^2)}$

Soundness $D = A \times B$

$C \neq D$

then $\exists i$ $c_i \neq d_i$ & $c_i \cdot \vec{r} = d_i \cdot \vec{r}$

$(c_i - d_i) \cdot \vec{r} = 0$

$(p_0, p_1 \ldots p_{n-1}) \cdot (1, r, \ldots r^{n-1}) = 0$

$p(x) = p_0 + p_1 x + p_2 x^2 \ldots p_{n-1} x^{n-1} \bmod q$

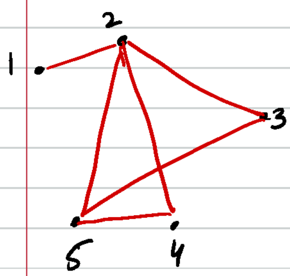
$p_0 + p_1 r + p_2 r^2 \ldots p_{n-1} r^{n-1} = 0 \Leftrightarrow p(r) = 0$

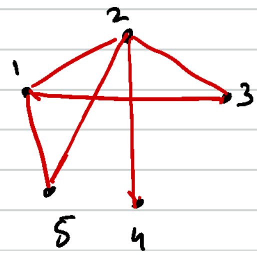
$O\left(\frac{n-1}{q}\right)$

Graph Isomorphism

Instance: $G_0 = (V, E_0)$ $\quad G_1 = (V, E_1)$ $\quad G_0 \cong G_1$

Solution: $\pi : V \to V$ s.t $\forall\, e = (u, v) \in E_0$ iff $(\pi(u), \pi(v)) \in E_1$





$1 \to 4$
$2 \to 2$
$3 \to 3$
$4 \to 5$
$5 \to 1$

Graph Non-isomorphism

$$G_0 \not\cong G_1$$

$H \to G_0$
$H \to G_1$

$P \xleftarrow{H = \sigma(G_b)} V$

$\xrightarrow{b'}$

V: ① $\sigma : \{V \to V\}$
② $b \leftarrow \{0, 1\}$

$b = b'$ then output 1
else output 0

Completeness: ✓

Soundness: $G_0 \cong G_1 \cong H$

$P \xleftarrow{H = \sigma(G_b) = \sigma'(G_{1-b})}$ $\quad \frac{1}{2^n}$

$\xrightarrow{b'}$ $\quad \Pr[b = b'] = \frac{1}{2}$

GI $\qquad G_0 \approx G_1$

$$P \xrightarrow{\quad \pi \quad} V$$

→ zero-knowledge: If $G_0 \approx G_1$ then V learns nothing more than the fact that $G_0 \approx G_1$

↳ V will be able to generate the interaction on his own.

→ G_0, G_1, π $\qquad\qquad\qquad\qquad$ G_0, G_1

P $\qquad\qquad\qquad\qquad\qquad\qquad$ V

1) $\sigma \leftarrow \{V \to V\}$ $\qquad$ ② $H = \sigma(G_1)$ $\longrightarrow$ $\qquad$ $b \xleftarrow{\$} \{0,1\}$

$\longleftarrow$ ① b

$b=1$ $\quad \phi = \sigma$ $\longrightarrow$ $\qquad$ if $\phi(G_b) = H$ then output 1

$b=0$ $\quad$ ③ $\phi = \sigma \circ \pi$ $\qquad\qquad\qquad\qquad$ else 0

Complete: $\quad G_0 \approx G_1 \approx H$

Soundness: $\quad G_0 \not\approx G_1$ $\qquad$ $H \to G_0$, $H \not\to G_1$ $\qquad$ $H \approx G_\beta$

with probability $\frac{1}{2}$ $\quad b \neq \beta$ then P will have no way to make V output 1.

Zero-knowledge: $\quad G_0 \approx G_1$

$\sigma \leftarrow \{V \to V\}$ $\qquad$ ② $H = \sigma(G_b)$ $\longrightarrow$

$\longleftarrow$ ① $b \leftarrow \{0,1\}$

③ σ $\longrightarrow$

$$\left.\begin{array}{c} \xrightarrow{H} \\ \xleftarrow{b} \\ \xrightarrow{\sigma} \end{array}\right] \approx \begin{array}{c} \xrightarrow{H} \\ \xleftarrow{b} \\ \xrightarrow{\sigma} \end{array}$$

$b \leftarrow \{0,1\}$

$\sigma \leftarrow \{V \to V\}$

$H \to \sigma(G_b)$

$\sigma \xleftarrow{\$} \{V \to V\}$

$H = \sigma(G_0) = \sigma'(G_1)$