Course evaluations — starting Monday — Dec 13

course-evaluations.berkeley.edu

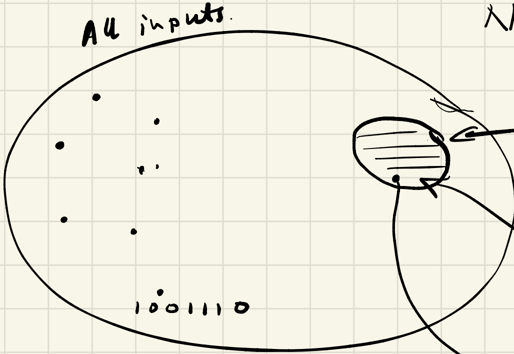
csec@hkn.mu

Final Exam: Dec 16 6–9 pm

---

* Coping with NP-completeness.
* Primality testing
* Hashing & Streaming algorithms
* Quantum algorithms.

NP-complete problem X:



{NPC means some really hard instances

Hard!!

answer $a_0 . a_1 a_2 a_3 \cdots \underbrace{\quad a_k}_{\text{hard!}}$

Heuristics: geometrical intuition
Nature!

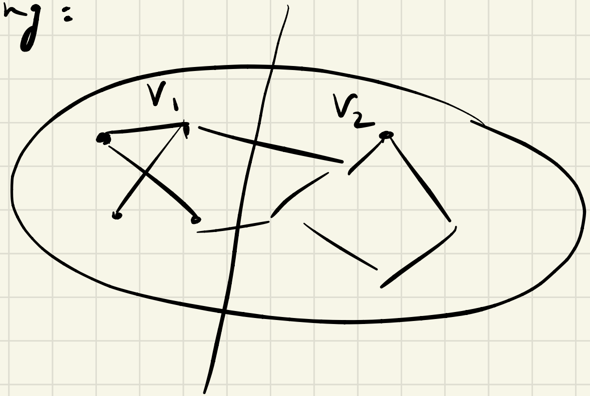
Graph partitioning:

Input: $G(V,E)$

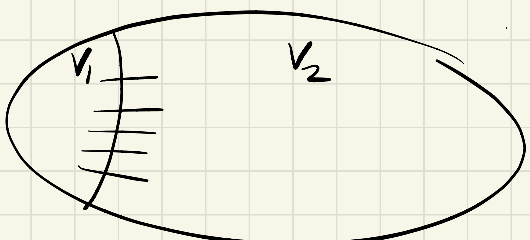
Goal: V_1, V_2

$$V_1 \cup V_2 = V$$
$$V_1 \cap V_2 = \phi$$
$$\frac{|V|}{3} \le |V_1| \le \frac{2|V|}{3}$$

Minimize # crossing edges.

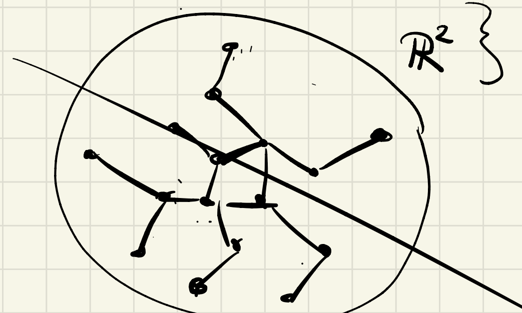


Normalized cut: V_1, V_2 : $\min \dfrac{|E_{V_1,V_2}|}{\min\{|V_1|, |V_2|\}}$.



minimize $\sum_{(u,v)\in E} d(u,v)^2$

line



unit disc

$\mathbb{R}^2 \Big\}$ suppose: $\min \sum_{\{u,v\}\in E} d(u,v)$

$$\sum_{u,v} d(u,v) = \binom{n}{2}$$

$\mathbb{R}^n$

Integer linear program:

LP $\longrightarrow$ rounding

Simulated annealing:

All potential solutions:

configuration $\longrightarrow$ $\underline{\underline{X}}$ $\longrightarrow$ $\underline{\underline{C(x)}}$ $\longleftarrow$ energy

min $C(X)$.

Temperature T

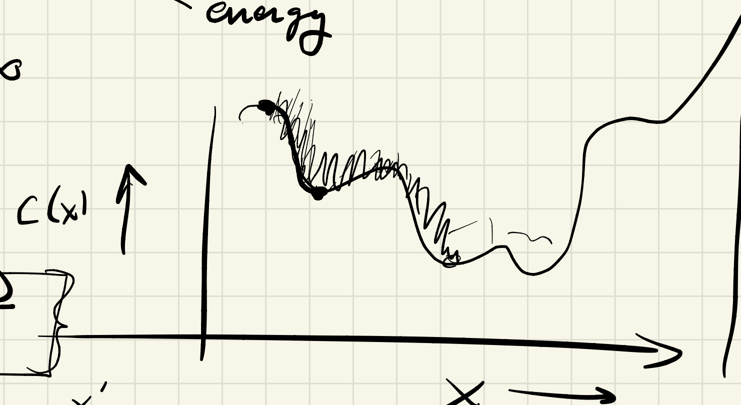
Start T high ∞

lower $\downarrow$

$T = 0$

$$\boxed{\text{Gibbs distribution} : \approx e^{-\frac{C(x)}{T}}}$$

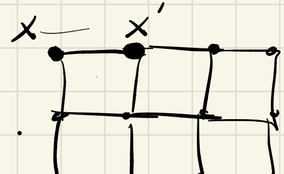
$T \approx 0$



$x' \longrightarrow x$

$E(x') > E(x)$ move to x.

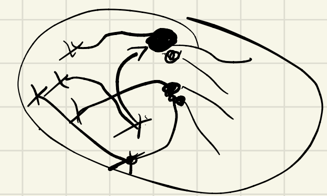
$E(x') < E(x)$ move to x $\boxed{\text{wp} \quad e^{-\Delta/T}}$



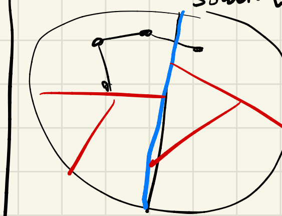
$\Delta = E(x) - E(x')$.

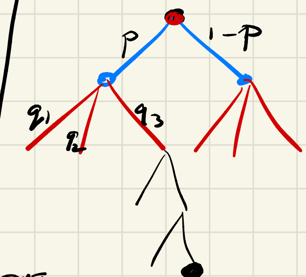
x, x' adjacent if differ in 1 coordinate.

Go with the winners heuristic.



SA





SAT

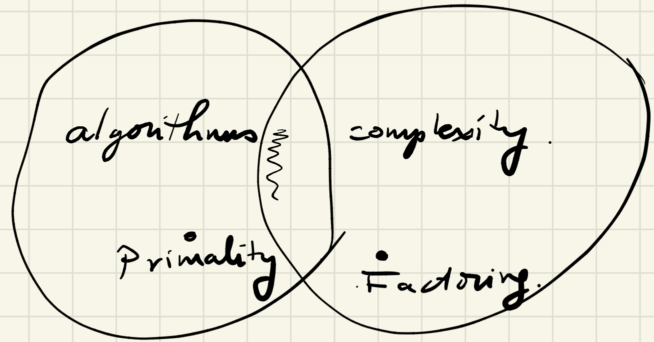
$f(x_1, \ldots, x_n)$

$= c_1 \wedge c_2 \wedge \cdots \wedge c_m$

x # unsat clauses

Primality testing: Is N prime?

1. Randomized algorithm
2. Hashing
3. Cryptography $\longleftrightarrow$



Factoring: Write $N = N_1 \cdot N_2$

Input: N
Output: N_1, N_2: $N_1 \cdot N_2 = N$
$N_1, N_2 \neq 1$.
or say not possible.

$35 = 5 \times 7$

N 1000 bit number.
$N \approx 2^{1000}$
$n = 1000$ length
Time: poly(n).

Fermat's Little Theorem: If N prime then

$\forall a \not\equiv 0 \bmod N$ $\quad \boxed{a^{N-1} \equiv 1 \pmod N}$

"Industrial grade": test $\quad 2^{N-1} \equiv 1 \pmod N$
$3^{N-1} \equiv 1 \pmod N$
$5^{N-1} \equiv 1 \pmod N$