Last time: continued unit on cxity of counting problems: FP, #P, #P-completeness, reductions, examples, permanent.

Papad. 18.1, AB 17.1–17.3

Today:
- show that PER of 0/1 matrices is in #P. (RSR)
- Random self reducibility: AB 8.6.2

PER's worst-case hardness ⇒ avg-case hardness.
- approximate counting (maybe)

Questions?

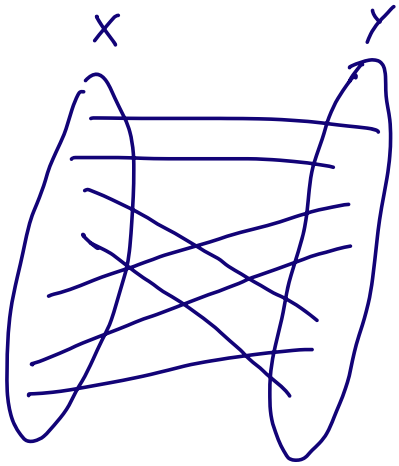
Consider PER on 0/1 matr.:

0/1 PER:
- input is $n \times n$ mtx M of 0/1 entries.
- output = PER(M)

Obs: The problem is ≡ to #PM (Perfect Matching)

Recall a PM in undir. graph G is a set S of edges s.t. each vtx in G touches exactly

one edge in S.



If G bipartite, poss. to have PM only if $|X| = |Y|$.

#PM: · input is bip. $G = (X \cup Y, E)$
· output is # of PMs in G.

Pf of Obs: Given ↓, construct adj. matrix: $M_{ij} = \begin{cases} 1 & \text{if } \exists\ X(i) - Y(j) \text{ edge} \\ 0 & \text{if } \nexists \text{ " " " " " " .} \end{cases}$

Each monom. in PER(M) is product of n 0/1 values: 1 iff all 1's; i.e. all the n cand. edges are in G; i.e. that monom. is in G.

So 0/1 PER is in #P.
We didn't "prove 0/1 PER is #P-hard, but it is (see book...)

PER nice for many reasons...

one: provable conn. between worst-case & average-case hardness, via random self-reducibility.

Informal riff on ↓ & ↓ hardness:

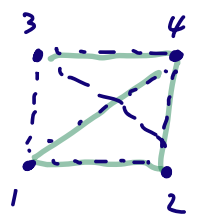
WC

"worst-case hardess": our usual notion:
any proposed poly-time alg is wrong on some inputs.

Very possible that a problem is WC hard, yet easy to solve on almost all inputs!

Ex: CUBE-ROOT-CLIQUE = {G: G is an n-node undir. graph that contains a $n^{1/3}$-size clique}. CRC is NPC; worst-case hard... but easy on random G.

- There are $2^{\binom{n}{2}}$ undir., no self-loop graphs G on n nodes.
- Unif. dist. over all these: a "random graph."

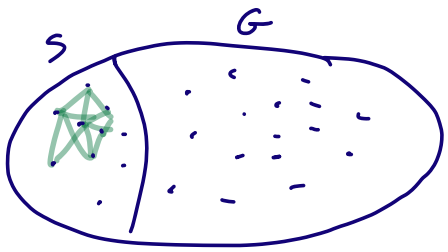


Consider a rand. G:

Claim: $\Pr[G \text{ cont. an } n^{1/3}\text{-clique}] \le \frac{1}{2^{\Theta(n^{2/3})}}$.

Pf: Fix any set $S \subseteq V$ of size $|S| = n^{1/3}$.

$$\Pr[S \text{ is a clique in } G] = \frac{1}{2^{\binom{|S|}{2}}} = \frac{1}{2^{\Theta(n^{2/3})}}$$



There are only $\binom{n}{n^{1/3}} \le n^{n^{1/3}} = 2^{n^{1/3}\cdot \log n}$ many poss. for S.

So by union bd,

$$\Pr[\underline{\text{any}} \text{ set of size } n^{1/3} \text{ is a clique in } G] \le 2^{n^{1/3}\cdot \log n} \cdot \frac{1}{2^{\Theta(n^{2/3})}} = \frac{1}{2^{\Theta(n^{2/3})}}. \quad \blacksquare$$

So CRC is very easy in avg. case: outputting "no" without even reading G, we have failure prob. $\le \frac{1}{2^{\Theta(n^{2/3})}}$.

So, a nat. question is: are there problems that are (presumably) worst-case hard + provably as hard in avg case as in worst case?

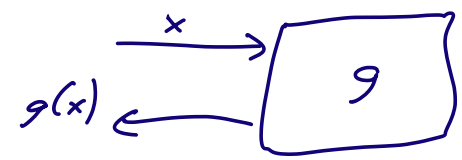
YES: PER.

Key idea for : RSR. Idea: "f is RSR":

- Suppose you can eff. compute f correctly on random instances (w.h.p. over instances) Then you can eff. compute f correctly using randomness on any specific x (w.h.p.), i.e. on worst-case instances.

→ Done by combining results of several comput. of f on random instances $y_1, \ldots, y_k$; each y_i rand., but y_i's related to each other in a particular way.

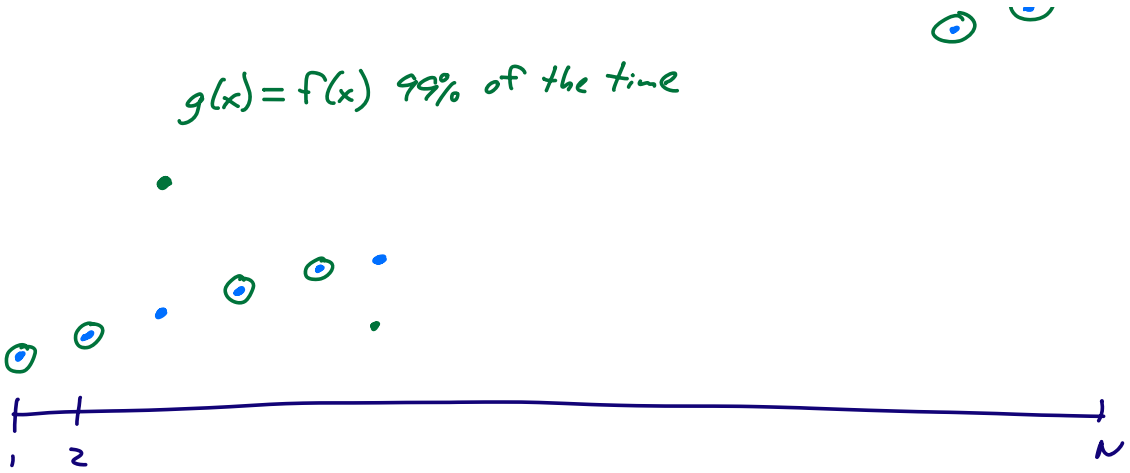
Ex: Suppose you have an oracle for a fn $g: \{1, 2, \ldots, N\} \to \mathbb{R}$.



Sps g is a "noisy linear function" that's 99% consistent with some unknown lin fn $f(x) = ax + b$:

on $\frac{99}{100} \cdot N$ input (we don't know which ones), have $g(x) = f(x) = ax + b$.

$f(x) = ax + b \ \forall x$



Our goal: compute the unknown "true" fn f on a partic. fixed input $z \in \{1, \ldots, N\}$, i.e. $a \cdot z + b$.

↳ may have been provided by an adversary...

Not a good idea to just output $g(z)$: if z is a "worst-case" input, it could be one of the 1% of error points. (if z were adversarially chosen).

The fix:

- pick two unif. random pts $i, j \in \{1, \ldots, N\}$; call g twice to get $g(i), g(j)$
- Assuming $g(i) = a \cdot i + b$

  $g(j) = a \cdot j + b$, can solve

to get a, b; then $a \cdot z + b$ = desired answer.

- $\Pr[g \text{ wrong on either } i \text{ or } j] \leq \frac{2}{100}$, so this alg. is correct w.p. $\geq \frac{98}{100}$, no matter what z is.

Since i, j random,

We did: worst-case easy $\Leftarrow$ avg-case easy

Contrapos: worst-case hardness $\Rightarrow$ avg-case hardness.

What's the magic? Alg. struc. of linear fns.

PER also has algebraic structure; can do something similar.

Now: PER.

Easier/cleaner to work mod p (p prime): all our math is over $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, mod p.
Can $+, -, \times, \div$ as usual.

MODPER: **Input:** (M, p)
M is $n \times n$ matrix over $\mathbb{Z}_p$, p a prime.
Output: PER(M) mod p.

Claim: MODPER is #P-hard. (If there is a poly(n)-time alg for MODPER, then there's a poly(n)-time alg for 0/1 PER.)

Pf: Let M be an input to O/I PER, i.e. an $n \times n$ O/I matrix; want to compute $PER(M)$.

Let $p_1, \ldots, p_n$ be first n primes that are $\geq n$. (Easy to find in poly(n) time.)

Run our hyp. MODPER alg on

$(M, p_1) \rightsquigarrow a_1 \qquad (PER(M) \bmod p_1) \equiv a_1$

$(M, p_2) \rightsquigarrow a_2$

$\vdots$

$(M, p_n) \rightsquigarrow a_n$

Use Chinese Remainder Theorem (CRT) to combine answers $a_1, \ldots, a_n$ to get $PER(M) \bmod (p_1 p_2 \cdots p_n)$.

Since $p_1 p_2 \cdots p_n > n^n > n!$,

& $PER(M) \leq n!$,

$= PER(M)$. ■

CRT: Given (a, A, b, B)

where $0 \leq a \leq A-1$

$0 \leq b \leq B-1$, & A, B relatively prime,

based on extended Euclidean alg for GCD

there's an eff. alg. to compute the unique value $c \in \{0, 1, \ldots, AB-1\}$ s.t.

$(c \bmod A) \equiv a$

$(c \bmod B) \equiv b$.

Ex: if $x \in \{0, \ldots, 343\}$ + $(x \bmod 7) \equiv 4$,
$(x \bmod 5) \equiv 2$,

must have $x = 32$.

So, MOOPER is (presumably) worst-case hard; next time: use RSR to show that it is as hard in the average case as in the worst case!
