Last time: • PER of 0/1 matrices is in #P.

RSR

• Random self reducibility:

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

$\equiv$ to

worst-case easiness $\Leftarrow$ avg-case easiness

AB 8.6.2

Today: • PER is RSR:

"avg-case easy" $\Rightarrow$ "worst-case easy"

(hence "worst-case hard" $\Rightarrow$ "avg-case hard").

• approximate counting

Questions?

Thm: Let $p > n+1$.

Suppose A is a poly(n)-time alg. that solves PER$_{n\times n}$ mod p correctly on at least a $1-\frac{1}{3(n+1)}$ frac. of all p^{n^2} many input matrices $M \in \mathbb{Z}_p^{n\times n}$.

Then there is a poly(n)-time rand. alg. A' s.t.: for any input matrix $M \in \mathbb{Z}_p^{n\times n}$, alg. A' correctly outputs PER(M) mod p w.p. at least $2/3$.

Pf: Let $M \in \mathbb{Z}_p^{n \times n}$ be any input mtx.

Our alg A' works like this:

① Choose unif. rand. mtx $R \in \mathbb{Z}_p^{n \times n}$ (each R_{ij} unif. rand. over $\mathbb{Z}_p = \{0, 1, \ldots p-1\}$)

② For $t = 1, 2, \ldots, n+1$, form mtx $M + t \cdot R$ & run A on it to get values $y_1, \ldots, y_{n+1}$; y_t = output of A on $M + tR$.

③ Use polynomial interpolation to find the (unique) degree-at-most-n univariate poly $p(t) = a_0 + a_1 t + \ldots + a_n t^n$ s.t. $y_t = p(t)$ for $t = 1, \ldots, n+1$.

④ Return $p(0) = a_0$.

Recall: given $(d+1)$ pairs of real #s $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$, where $x_1, \ldots, x_{d+1}$ all different, there is a unique poly p of deg $\leq d$ s.t. $p(x_i) = y_i$ $\forall i = 1, \ldots, d+1$. Can find p efficiently (lin. algebra). Can do over $\mathbb{Z}_p$ as well.

Analysis:

Claim 1: For each $t = 1, \ldots, n+1$, the matrix

$M + tR$ is unif. rand. over $\mathbb{Z}_p^{n \times n}$.

Consider the (i,j) entry:

$$M_{ij} + t \cdot R_{ij} = \alpha \quad \text{iff} \quad R_{ij} = \frac{\alpha - M_{ij}}{t}$$

(ok; $p > n+1$, $t = 1, \ldots, n+1$; no div. by 0)

Same arg. works even for all n^2 (i,j) pairs simult.

Claim 2: W.p. $\geq 2/3$, each y_t (what A returned on $M+tR$) is actually equal to $PER(M+tR)$.
(union bd over $n+1$ fail prob., each $\leq \frac{1}{3(n+1)}$).

Claim 3: For any fixed M, R, $PER(M+tR)$ is a deg-at-most-n univ. poly in t. $\leq p(t)$

Comb. C2 + C3, w.p. $\geq 2/3$, step 3 of alg finds poly $p(t) \leq PER(M+tR)$.

Claim 4: W.p. $\geq 2/3$, $p(0) = PER(M + 0 \cdot R) = PER(M)$. ■

Backbone: naive poly. interp. (Berlekamp)

Via more sophisticated arg. (non-naive), can replace $1-\frac{1}{3(n+1)}$ w/ (essentially) $\frac{1}{2}$.

Even more: if $p > n^{2k}$, can replace $1-\frac{1}{3(n+1)}$ with $\frac{1}{n^k}$.

Last part of counting unit: approximate counting.

Motivation:
- exact counting often hard...
- ↓ ↓ ↓ unnecessary...

"Counting": often cleaner to normalize s.t. all counts are in $[0,1]$.

length-k paths: $[0, n^k]$
s.a. of $\varphi(x_1,\dots,x_m)$: $[0, 2^m]$
Ham. cycles: $[0, (n-1)!]$

---

2 notions of "approximate".
Consider #3CNF: given formula φ, n-var

let $p := \frac{\#\text{s.a. of } \varphi}{2^n} \in [0,1]$.

An estimate p' of p has

- <u>additive/absolute error ε</u> if

$$p - \varepsilon \le p' \le p + \varepsilon \quad ;$$

- <u>multiplicative/relative error ε</u> (same as add. approx. $p\varepsilon$) if

$$(1-\varepsilon)p \le p' \le (1+\varepsilon)p$$

Additive error easier/weaker (to achieve).

A trivial rand. alg. yields a good absolute-error approx. for any counting problem.
Consider #3CNF:

alg is:
- draw m unif. rand. inputs in $\{0,1\}^n$
- let p' = frac. of these m pts that sat. the input formula

Chernoff bound: if $m = \log(2/\delta)/\varepsilon^2$, then w.p. $\ge 1-\delta$, p' is in $[p-\varepsilon, p+\varepsilon]$.

[if you want det alg, it's interesting to find eff additive approx. algs.]

We focus on rel. error; we allow randomness.

Def: Let $f : \Sigma^* \to \mathbb{N}$ be a function. Let $0 < \varepsilon < 1$.
An alg A is a (randomized) ε-approx. alg for f if $\forall x$,

$$\Pr\left[(1-\varepsilon) f(x) \le A(x) \le (1+\varepsilon) f(x) \right] \ge 2/3$$

(A's input is x, ε).
If A's runtime is $\text{poly}(|x|, \frac{1}{\varepsilon})$, we say A is an FPRAS
(fully poly. rand. approx. scheme).
[other poss: A's runtime is $n^{\frac{1}{\varepsilon}}$, $n \cdot 2^{\frac{1}{\varepsilon}}$, $n^{2^{\frac{1}{\varepsilon}}}$]

Fact: ε-Approx counting, for $0 < \varepsilon < 1$, is as least as hard as decision.

So, shouldn't expect ε-approx. counting for

problems (like 3CNF-SAT) for which decision is hard.

What about problems (like #DNF) where decision is easy - can we do approx. counting? Sometimes Y, sometimes N (#DNF, #CYCLES.)

Thm: There is an FPRAS for #DNF.

Let f = input = $T_1 \vee \dots \vee T_s$, an s-term DNF over $x_1, \dots, x_n$ (we'll assume no T_i has any $x_j \wedge \bar{x}_j$)

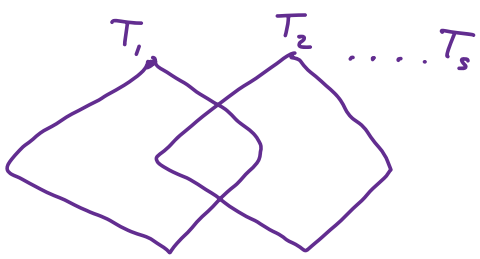
Let t_i = length of T_i; e.g.

$T_1 = x_1 \wedge x_3 \wedge x_4 \wedge \bar{x}_5$, $t_1 = 4$.

$T_2 = x_2 \wedge \bar{x}_3 \wedge x_4$

s.a. of $T_i = 2^{n-t_i}$.

Want to output $p' \in [p(1-\varepsilon), p(1+\varepsilon)]$ where $p = \frac{\#\text{ s.a. of } f}{2^n}$.



First naive approach:

- inclusion/exclusion.

Let's write $|T_i|$ for # assts in $\{0,1\}^n$ that sat. T_i.

tot # s.a. $= |T_1| + \ldots + |T_s| - |T_1 \cap T_2| - |T_1 \cap T_3|$
$\ldots - |T_{s-1} \cap T_s| + |T_1 \cap T_2 \cap T_3| + \ldots$

2^s terms in sum $\rightsquigarrow$ No good.

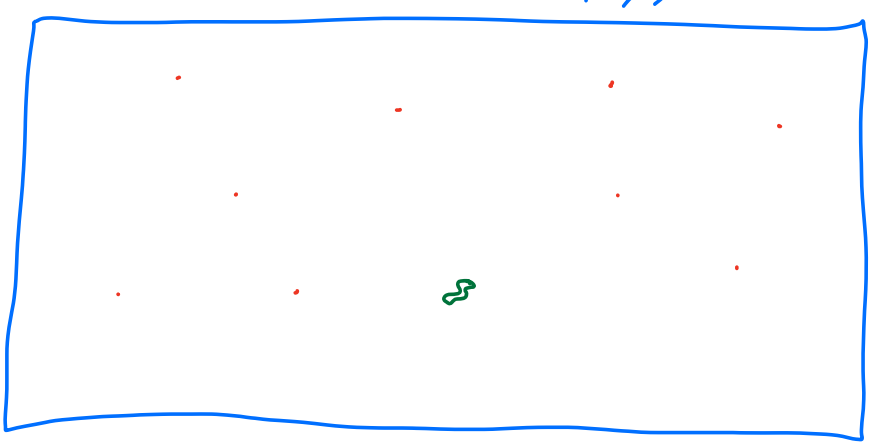
Second approach: unif. rand. sampling, like above.

Problem: need $\pm p\varepsilon$ accuracy, i.e.
$\approx \frac{1}{(p\varepsilon)^2}$ many samples; could be huge.

Suppose each T_i has $t_i \geq \frac{n}{3}$.
Then true frac p of s.a. is $\leq s \cdot \frac{1}{2^{n/3}}$;
tiny

. = rand. pt in $\{0,1\}^n$

$\{0,1\}^n \to 2^n$

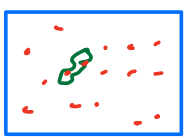


$\S$ = the sat. assts of f.

Rand. sampling ineff; almost never hit target region.

Idea: If could create a small box cont. of known area

" sample from small box uniformly,



→ if I know area can sample.

→ s.t. target is nontrivial fraction of little box

→ then we could make rand. sampling.

Next time we'll make this rigorous.