**Last time:** • PER is RSR:

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

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

• started approximate counting:

basics (absol./rel. error); FPRAS; started FPRAS for #DNF.

**Today:**

- FPRAS for #DNF: alg + proof
- hardness of approx. #CYCLES
- sketch of FPRAS for any fn in #P (provided we have an NP-oracle)
- coming up: communication complexity... AB 13.1, 13.2

**Admin:** PS3 due; PS4 out (5 extra days for it :) )

**Questions?**

Recall we're giving an FPRAS for # s.a. of $f = T_1 \vee \dots \vee T_s$.

Let • $A \subseteq \{0,1\}^n$: $A$ = set of s.a. of $f$.

(Goal: estimate $|A|$.)

- $U = \{(x,i) : \quad T_i(x) = 1\}$

  ↳ coll. of all pairs (asst, term which sat.)
  (x's in $U$ are same as pts in $A$)

- $B = \{(x,i) \in U : (x,j) \notin U \text{ for } j < i\}$

  ↳ coll of all pairs (asst, <u>1st</u> term which sat.)
  (x's in $B$ are same as pts in $A$)

Input is $T_1, \ldots, T_s$

Given $x, i$, easy to figure out whether $(x,i) \in B$ (check $T_i(x) = 1$, $T_1(x) = \ldots = T_{i-1}(x) = 0$).

<u>Fact 1:</u> Have $|B| = |A|$.

True b/c each $x \in A$ has some ! term $i$ that's the first term it sat.; have $(x,i) \in B$; don't have $(x,i') \in B$ for any other $i'$; & this is all of $B$.

<u>Fact 2:</u> Have $|U| \le s \cdot B$.

True b/c each $(x,i) \in B$ corr. to some s.a. $x$ (these are all the s.a.'s), & each such $x$ sat. $\le s$ terms, hence $\le s$ many $(x,j)$'s in $U$ for that $x$.

Ex: if x sat. $T_2$, $T_5$, $T_7$, have

$(x,2) \in B$

$(x,2)$, $(x,5)$, $(x,7)$ all $\in U$.

$t_i = \#$ lits in $T_i$

**Fact 3:** Easy to exactly compute $|U|$:

$2^{n-t_i} = |T_i|$

$$|U| = 2^{n-t_1} + 2^{n-t_2} + \dots + 2^{n-t_s}.$$

**Fact 4:** Easy to sample unif. rand. elt of $U$:

first (a) pick $i \in \{1, \dots, s\}$ w.p.

$$\frac{2^{n-t_i}}{(2^{n-t_1} + 2^{n-t_2} + \dots + 2^{n-t_s})}$$

(b) once have $i$, fix bits in $T_i$ s.t. they satisfy $T_i$, & toss fair coin for each of $n-t_i$ other vars.

Ex: if $i = 4$ & $T_4 = x_2 \wedge \overline{x_5} \wedge x_6$,

fix $x_2 = 1$

$x_5 = 0$

$x_6 = 1$

$\underline{\$}\ 1\ \underline{\$}\ \underline{\$}\ 0\ 1\ \underline{\$}\ \underline{\$}\ \underline{\$}$

Alg to est. # s.a. of (i.e. $|A|$) :

repeat $M$ times:

- choose unif rand elt of $\mathcal{U}$
- if belongs to $B$, "succeed" else "fail"

Let $Y$ = # of "succeed"

Our estimate is $\underbrace{|\mathcal{U}|}_{\text{we compute this}} \cdot \underbrace{\frac{Y}{M}}_{\text{frac. of "succeed" we saw}}$

<u>Analysis:</u>

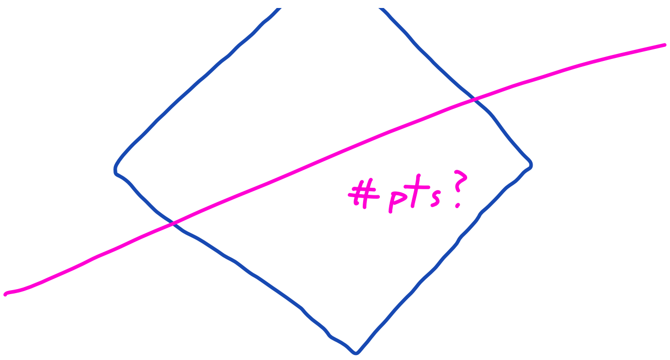
$\Pr[$ a fixed repetition gives "success" $] = \frac{|B|}{|\mathcal{U}|} \geq \frac{1}{s}$.

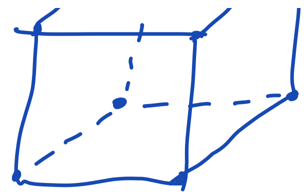
CB $\Rightarrow$ if $M = \frac{\log(2/\delta) \cdot s}{\varepsilon^2}$ then w.h.p. $1-\delta$

our obtained estimate $\frac{Y}{M}$ will satisfy

$$(1-\varepsilon)\frac{|B|}{|\mathcal{U}|} \leq \frac{Y}{M} \leq (1+\varepsilon) \cdot \frac{|B|}{|\mathcal{U}|}$$

So $|\mathcal{U}| \cdot Y/M$ is as desired.

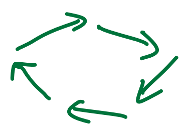




So #DNF: dec. easy :), approx count easy :)

#CNF: dec hard :(, hence hard :(

Anything in Middle? Yes:



input: digraph G; cycle

#CYCLES: dec easy :), approx count hard :(

BFS, DFS

Output # of directed cycles in G.

**Fact**: #CYCLES is #P-hard.

**Thm**: If there is a det (rand) poly-time $\frac{1}{2}$-approx alg. for #CYCLES, then $NP \subseteq P^{RP}$.

**Pf**: "blowup".

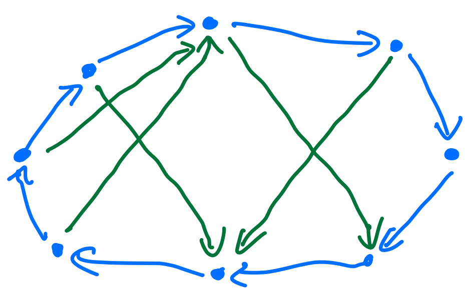
Sps there is a (poly-time) $\frac{1}{2}$-approx alg for #CYCLES.

We'll use it to give a poly-time alg to solve

HAM CYCLE (NP complete.)

↳ input: digraph of $n$ nodes

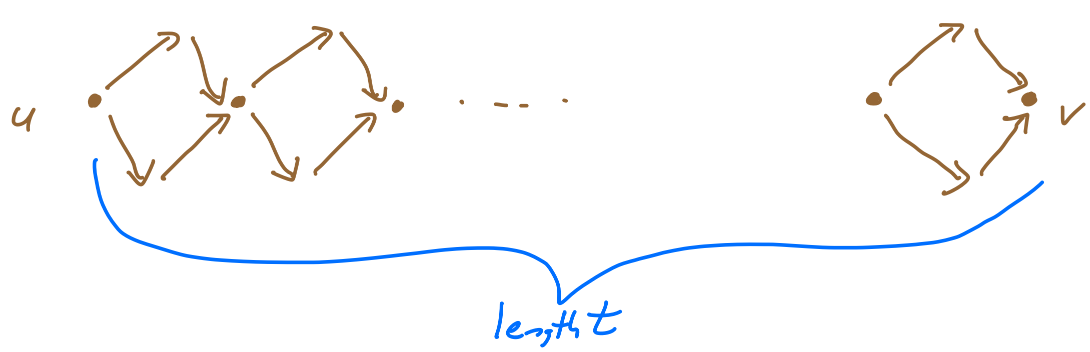
q: does it have a "Ham cycle" (cycle of length $n$ going thru each node exactly once)



Input digraph $G$ (does $G$ have HC?)

For each $e = u \to v$ in $G$, "blow it up"

i.e. replace with




Call this graph $G'$.

Any $u \longrightarrow v$ journey in $G \rightsquigarrow 2^t$ poss. paths in $G'$

So

any length-$k$ cycle in $G \rightsquigarrow 2^{tk}$ cycles in $G'$.

So

(n nodes)

- if $G$ has a HC, then $G'$ has $\geq 2^{tn}$ cycles

- if $G$ has no HC, then each cycle in $G$ blown up to $\leq 2^{t(n-1)}$ cycles.

$G$ had $\leq n! < n^n$ cycles

So if $G$ has no HC, then tot # cyc. in $G'$ is

$$\leq n^n \cdot 2^{t(n-1)}.$$

Take $t = n^2$. Then

$$\text{ratio } \frac{(\#\text{ cyc in } G' \text{ if } G \text{ had a HC})}{(\#\text{ cyc in } G' \text{ if } G \text{ had no HC})}$$

$$\geq \frac{2^{tn}}{n^n \cdot 2^{t(n-1)}} = \frac{2^{n^3}}{n^n \cdot 2^{n^3-n^2}} = \frac{2^{n^2}}{n^n} = 2^{n^2 - n\log n}$$

$$\geq 2^{n^2/2}$$

So if could est #cycles in $G'$ to $\frac{1}{2}$-factor, could figure out whether or not $G$ had a HC. ∎

---

Just saw: approx. count #cycles is "as hard as NP".

Turns out: <u>every</u> approx. count problem "no harder than NP": given an NP oracle, can solve any approx. count problem in poly time!

<u>Thm:</u> Fix any $g \in \#P$. There is an FPRAS for $g$ which uses an oracle for NP (SAT oracle).

<u>Sketch:</u> 3 basic ingredients.

---

1) Enough to give FPRAS for #3CNF:
given any $g \in \#P$, can run the 2 parsinonious reduc's we saw
(Cook-Levin: NTM for $g \rightarrow$ CKT-SAT
: CKT-SAT $\rightarrow$ 3CNF SAT )
So approx. #3CNF $\equiv$ approx. $g$.

2) FPRAS: $(1 \pm \varepsilon)\cdot$ approx to #3CNF.

HW: prove that if $A$ is a "coarse" poly-time approx alg for #3CNF, meaning on input formula $\varphi$, $A$ satisfies

$$\frac{1}{100} \cdot (\#\text{s.a. to } \varphi) \le A(\varphi) \le 100 \cdot (\#\text{ s.a. to } \varphi)$$

or even

$$\frac{1}{n^2} \cdot (\#\text{s.a. to } \varphi) \le A(\varphi) \le n^2 \cdot (\#\text{ s.a. to } \varphi),$$

then there's an alg $A'$ that is an FPRAS.

So suff. to just come up with a "coarse" 100-approx alg.

---

3) Can use NP oracle + randomiz. to get poly-time "coarse" approx. alg.

---

Pile of sand. approx # grains?

Repeat:

- take half the sand (approx), throw it away
- is any sand left? if so, repeat.

Do this $k$ times, then no sand left.

Could plausibly guess "$\approx 2^k$ grains" in orig. pile.

---

sand = s.a. of $\varphi$.

Take new $\varphi_1 = \varphi \wedge h_1$

rand hash fn; keeps $\approx \frac{1}{2}$ of all of $\varphi$'s s.a.'s

- run $\varphi_1$ thru NP oracle (is $\varphi_1$ satisfiable?)

if so, repeat: $\varphi_2 = \varphi_1 \wedge h_2$ etc

---

Next time: comm cxity.