LECTURE 22

Note Title 5/2/2007

TODAY:

- A DNP-Complete Problem under "uniform" distribution

[Impagliazzo-Levin]

Goal of lecture

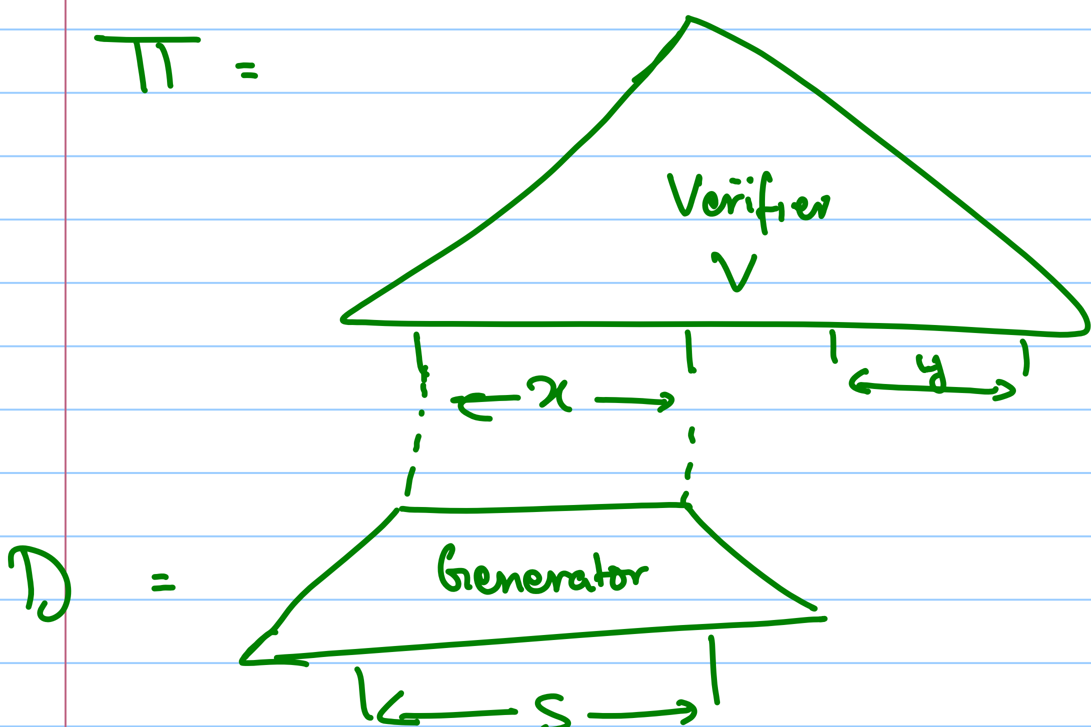
"Reduce" $(\Pi, D) \longrightarrow (\tilde{\Pi}, U)$

↑ Sampleable distribution.

In the process: ① What is a reduction?

② What is uniform?

Examining what is given



Need algorithms R, T, $\tilde{\Pi}_{verifier}$:

$$\begin{tikzcd}
x \arrow[r, "R"] \arrow[d, leftrightarrow] & R(x) \\
T(y) & y' \arrow[l, "T"'] \arrow[u, "\tilde{\Pi}_{verifier}"']
\end{tikzcd}$$

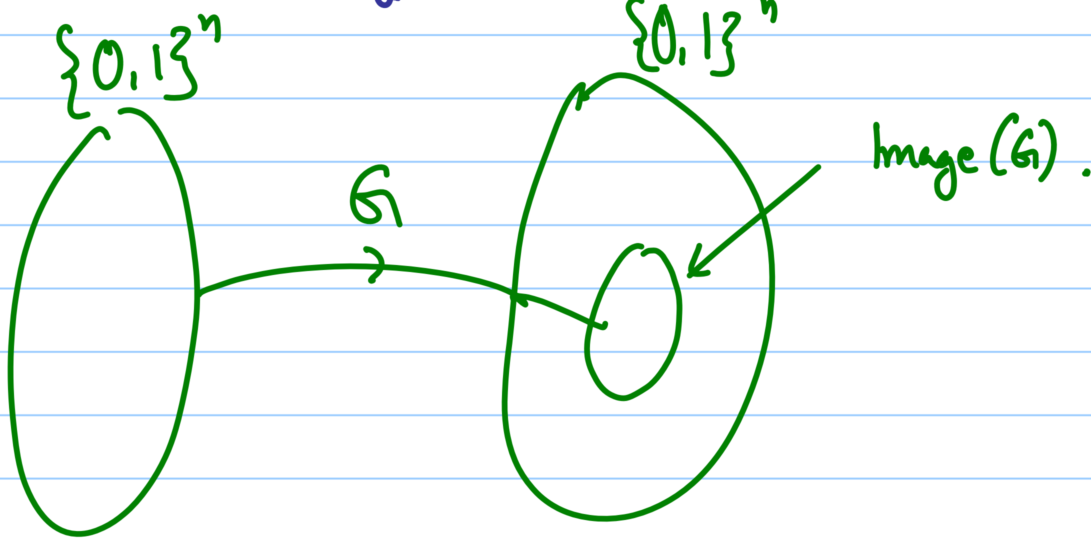
Wish : "$R(x)$" uniform

Trivial Case : G is 1-1 on $\{0,1\}^n$.

Then $R = T =$ Identity ;
$\tilde{\Pi} = \Pi$ work.

$R(x) = R(G(s)) =$ uniform .

Slightly more interesting : G is 2^ℓ to 1 .



What should $R(x)$ do ?

Don't know how to specify s st $G(s) = x$.

Idea: Hash "$\mathrm{Im}(G)$" to $\{0,1\}^{n-\ell}$.

Hopefully: 1-1 ;

if so $h(x) =$ uniform on $\{0,1\}^{n-\ell}$.

$$x \xrightarrow{z = h(x)} (h, z)$$

$$\tilde{\pi} = ?$$

$$\xleftarrow{T = ?}$$

$$\tilde{\Pi}\Big((h, z),\ (s', x', y')\Big) = 1 \quad \text{if}$$

"$G(s') = x'$"

and "$h(x') = z$"

and "$\Pi(x', y') = 1$"

$$T\big(x,\ (s', x', y')\big)$$

$= y'$ if $x' = x$

$= \bot$ ("not found") otherwise

Analysis

- Let A be "Avg. BPP" alg. for $(\tilde{\Pi}, U)$

$$\Pr_{(h,z)}\left[\, A(h,z) \text{ incorrect} \,\right] \leq \delta < \frac{1}{n^c}.$$

- h <u>bad</u> for x if

$$\exists\, x' \neq x \in \mathrm{Im}(G) \text{ s.t. } h(x) = h(x').$$

$$\Pr\left[\, h \text{ \underline{bad} for } x \,\right] \leq \frac{1}{2}.$$

- Dist. $\big(h, h(G(s))\big)$ dominated by Dist (h, z).

fix h_0, z_0

Claim: $$\Pr_{h,s}\left[\begin{array}{l} h = h_0 \ \& \\ h(G(s)) = z_0 \end{array}\right] \leq \alpha \cdot \frac{1}{|H|} \cdot \frac{1}{2^{n-\ell}}$$

Proof:

$$\Pr\left[h = h_0\right] = \frac{1}{|H|}$$

$$\Pr_{S}\left[h_0(G(S)) = z_0 \,\middle|\right.$$

Full Case: What else can go wrong?

- $|\mathrm{Im}(G)|$ may be unknown.
- # preimages in G of x may vary (for different x's) & unknown.

Idea:

- Guess ℓ $\approx \log|\mathrm{Im}(G)|$, k_x s.t.

$$\left|\{s \mid G(s) = x\}\right| \approx 2^{k_x}$$

- Use hash functions to uniquely specify a pre-image of x.

$R(x)$:
- Guess ℓ, k
- Pick $h: \{0,1\}^n \to \{0,1\}^{n-\ell}$ from p.w.i. family.
- Pick $\tilde{h}: \{0,1\}^n \to \{0,1\}^k$
- Pick $w \in_U \{0,1\}^k$
- $R(x) = (\ell, k, h, \tilde{h}, h(x), w)$

$\tilde{\Pi}((\ell, k, h, \tilde{h}, z, w), (s', y')):$

(i) $h(G(s')) = z$

and (ii) $\tilde{h}(s') = w$

and (iii) $\Pi(G(s'), y') = 1$

$T(x, (s', y'))$:

if $G(s') = x$ then y'

else $\perp$

Analysis:

- $\Pr[\underbrace{(\ell, k, h, \tilde{h}, z, w)}_{\text{uniform}}$ bad for $A] \leq \delta$

- D_2 = Uniform $(\ell, k, h, \tilde{h}, z, w)$

D_2' = $s \leftarrow$ uniform ; $(\ell, k, h, \tilde{h}, h(G(s)), \tilde{h}(s))$

D_2 α-dominates D_2'

(more leftover hashing).

- $\Pr\Big[$ (Guesses right) &

$h(G(s))$ & $\tilde{h}(s)$

uniquely specify $s \Big] \geq \frac{1}{\text{poly}}$.

<u>Conclude</u>: if x has match y under Π

thus reduction (R, T) produces such a

y w.p. $\geq \frac{1}{\text{poly}} - \alpha \cdot \delta$.

$\tilde{\Pi}$?

- Not as natural as promised in last lecture.
- But don't need to specify $\tilde{\Pi}$.
- Instead can pick relation $\tilde{\Pi}_i$ at random (w.p. $\sim \frac{1}{i^2}$) & it is the one of interest with $\Omega(1)$ probability.
- Final reduction ... given string

  $x \in \{0,1\}^n$, parse $x = (\langle m \rangle, x')$

  $\langle m \rangle$ - "prefix free" encoding of integer.

[• "Prefix free" encoding of integer

$$b_1 b_2 \ldots b_\ell$$

$$= b_1 b_1 \; b_2 b_2 \ldots \; b_{\ell-1} b_{\ell-1} \; b_\ell \bar{b}_\ell$$

(No prefix encodes another integer)]

Task: Solve M on x'.

[For our relation $\tilde{\Pi}$ of interest:

Parse $x' = (\underbrace{n, k, \ell}_{\text{Prefix-free.}}, h, \tilde{h}, z, w)$

& apply $\tilde{\Pi}$ to $(k, \ell, h, \tilde{h}, z, w)$:]

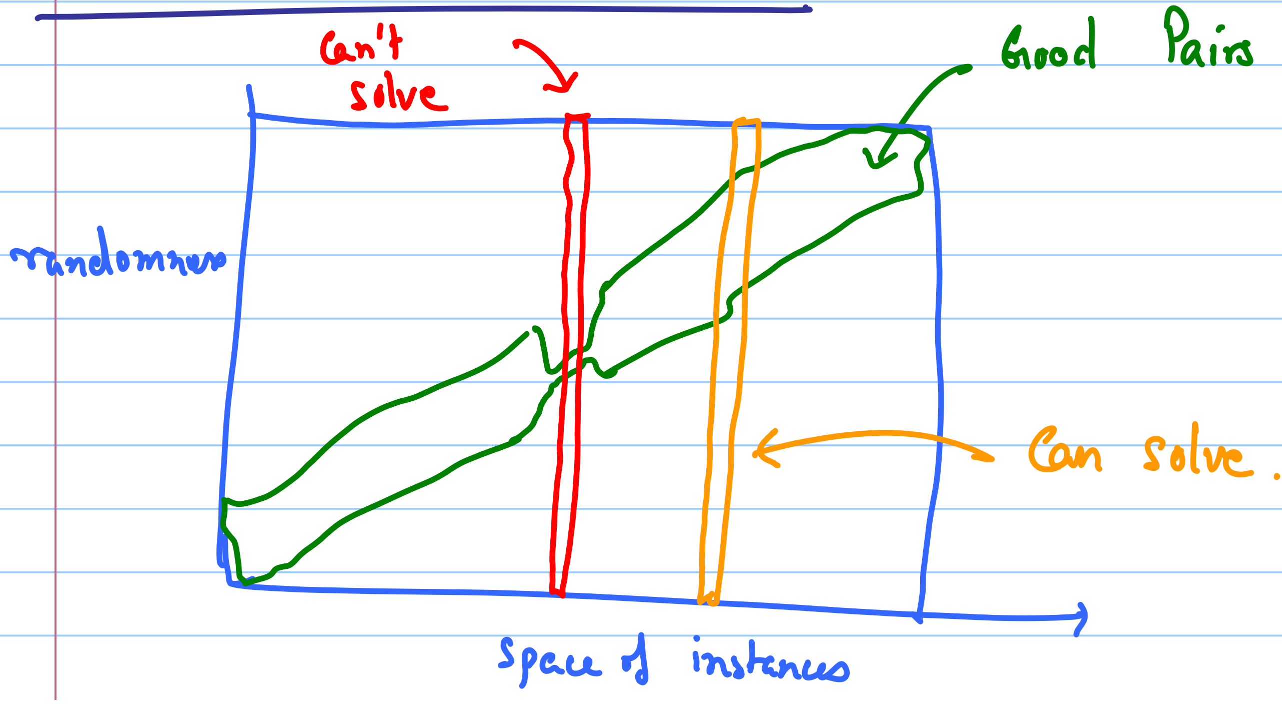
Is this uniform?

What else would be uniform?

Is this natural?

Still debated.

What is a reduction?



- Column is Red if density of good pairs is small
- Column is Orange if density of good pairs is $\geq \frac{1}{\text{poly}}$.
- Need Prob. of Red columns under distribution of instances to be negligible
- "Good Pairs" induce distribution on target dominated by target distribution.

(Complex. : See [Goldreich]).