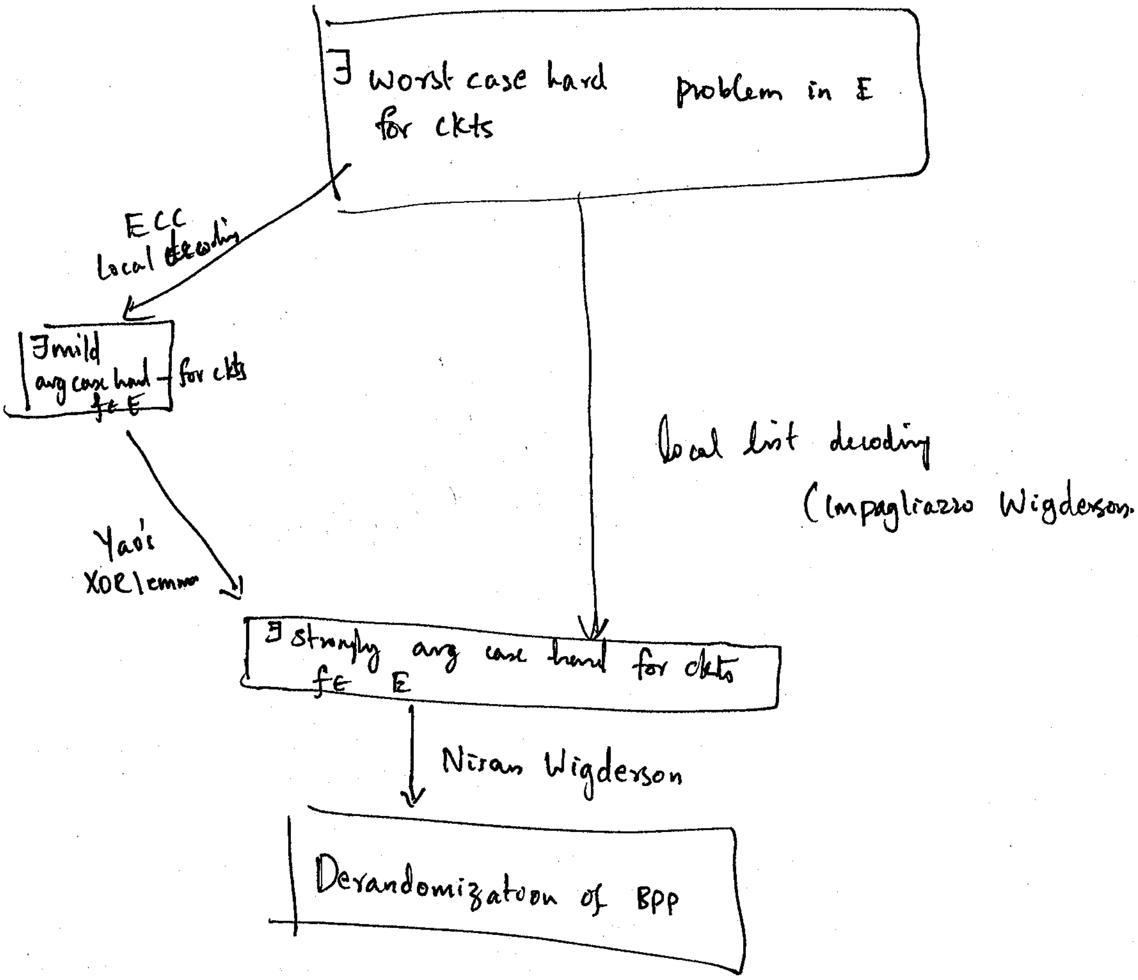
Impagliazzo's five worlds

Algorithmica	P=NP or NP=PPT
Heuristica	NP problems are worst case hard but easy on average.
Pessiland	NP problems are hard on average <u>yet</u> no one way functions exist.
Minicrypt	OWF exist but we do not have public key cryptography
Cryptomania	Public key cryptography exists.

Russell Impagliazzo, "A Personal view of Average-Case Complexity" - CCC 1995

Liu-Pass ~~on~~ 20+22, in particular, rules out Pessiland.


∃ worst case hard for ckts problem in E
ECC
Local decoding
∃ mild avg case hard f∈E for ckts
Yao's XOR lemma
local list decoding
(Impagliazzo Wigderson
∃ strongly avg case hard for ckts f∈E
Nisan Wigderson
Derandomizatoon of BPP

Definition

For $f : \Sigma^n \to \Sigma$, $\rho \in [0,1]$, we define the ρ-average case hardness of f, denoted $H_a^{\rho}(f)$ is

$$\max \{ S \mid \text{for every } \boxed{\text{circuit}} \text{ of } \boxed{\text{size}} \leq S \quad \Pr_{x \sim U_n} [C(x) = f(x)] < \rho \}$$

(every ckt of size S fails on at least $(1-\rho)$ fraction)

For $f : \Sigma^{\boxed{*}} \to \Sigma$, $H_a^{\rho}(f)(n) = H_a^{\rho}(f \restriction n)$ where $f \restriction n$ is the restriction of f to Σ^n.

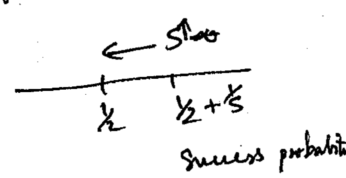
The worst-case hardness of $f : \Sigma^n \to \Sigma$ is $H_w(f) \triangleq H_a^{1}(f)$

(every ckt of size S fails on at least one input in Σ^n).

The average-case hardness of $f : \Sigma^n \to \Sigma$ is $H_a(f) \triangleq$

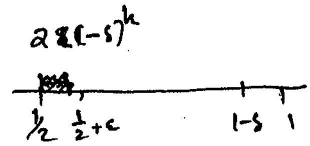
$$\max \{ S : H_a^{(\frac{1}{2} + \frac{1}{S})}(f) \geq S \}$$

(every ckt of size S fails on at least $1 - \frac{1}{2} - \frac{1}{S} = \frac{1}{2} - \frac{1}{S}$ fraction. On $S \uparrow$, $\frac{1}{S} \downarrow$, so the allowed failure fraction gets larger - i.e. the required success prob gets smaller and closer to $\frac{1}{2}$ from the right.)



The above formulation uses average-case hardness only over $\boxed{U_n}$.

Impagliazzo Hardcore Predicate



Theorem (Yao's XOR lemma)

$\forall f \in B_n \quad \forall \delta > 0 \quad \forall k \in \mathbb{N}$

$$\varepsilon > 2(1-\delta)^k \Rightarrow H_a^{\frac{1}{2}+\varepsilon}\left(f^{\oplus k}\right) \geq \frac{\varepsilon^2}{400n} H_a^{1-\delta}(f)$$

where $f^{\oplus k}: \Sigma^{nk} \to \Sigma$ is defined by $f(x_1, \dots, x_k) = \bigoplus_{i=1}^{k} f(x_i)$,

$x_i \in \Sigma^n$.

(e.g. if $\delta = 0.1$, $H(x) < \frac{10}{2^n}$)

Theorem (Impagliazzo Hardcore lemma)

A distribution H over Σ^n has density $\delta > 0$ if $\forall x \in \Sigma^n \quad H(x) \leq \frac{1}{\delta 2^n}$.

For every $\delta > 0$, $f: \Sigma^n \to \Sigma$ and $\forall \varepsilon > 0$

$H_a^{1-\delta}(f) \geq S \quad \Rightarrow \quad \exists$ density δ distribution H on Σ^n s.t. $\forall C$ of size $\leq \frac{\varepsilon^2}{100n} S$

$$\Pr_{x \sim H}\left[C(x) = f(x)\right] \leq \frac{1}{2} + \varepsilon$$

i.e. $H : \{x \in \Sigma^n \mid C(x) = f(x)\} \leq \frac{1}{2} + \varepsilon$.

Knuth says that it is a multiset.
The above notation is that of a set.
We sample again and again, with replacement.

The content of the Impagliazzo hardcore lemma is the following:

If a function $f: \Sigma^n \to \Sigma$ is hard on average, then it can either be

ⓐ unif hard on almost all instances

ⓑ extremely hard on a few instances, but may even be easy on others.

Impagliazzo's hard core lemma says that every strongly hard function $f: \Sigma^n \to \Sigma$ must be of type ⓑ.

Proof of Yao's theorem from Impagliazzo's lemma.

Proof overview:

Contra positive: $\neg Yao \Rightarrow \nexists\ \delta$ density distribution.

Proof:

Assume $f: \Sigma^n \to \Sigma$ be a function $H_a^{1-\delta}(f) \geq S$. Suppose, $\exists C$ with size $< \frac{\varepsilon^2}{400n} S$ such that

$$\Pr\left[C(x_1, \dots, x_k) = \sum_{i=1}^{k} f(x_i) \pmod 2 \,\middle|\, (x_1, x_2, \dots, x_k) \sim U_n^k\right] \geq \frac{1}{2} + \varepsilon \quad (1)$$

Contrary to the statement of Yao's XOR Lemma. We show that then this violates Impagliazzo's lemma. — for every δ, there is no density δ distribution H on Σ^n such that $\Pr\left[C(x) = f(x) \mid x \sim H\right] \leq \frac{1}{2} + \varepsilon$ for $\frac{\varepsilon^2}{100n} S$ circuits.

In other words, $\forall S, \exists C$ with size $\le \frac{\varepsilon^2}{100n} S$ such that — (2)

$$\Pr[C(x) = f(x) \mid x \sim H] > \frac{1}{2} + \varepsilon.$$

Let δ be the density and H be the hardcore density-δ distribution obtained from IHT, on which every $S' \triangleq \frac{\varepsilon^2}{400\,n} S < \frac{\varepsilon^2}{100n} S$ fails to compute f with probability $> \frac{1}{2} + \frac{\varepsilon}{2}$.

We can think of picking an element uniformly from Σ^n as follows: first toss a coin where the probability of heads is δ

- H: Pick a random element acc. to H
- T: " G

where G puts the "excess weight" on x:

$$G(x) = \frac{\left(\frac{1}{2^n} - \delta \Pr[H=x]\right)}{1-\delta}.$$

G is a distribution:

~~$G(x) = \frac{1}{2^n} - \frac{\delta \Pr[H=x]}{1-\delta}$ $\forall x\; \frac{1}{2^n} - \frac{\delta}{1-\delta} \cdot \frac{1}{\delta 2^n}$~~

~~$\frac{1}{2^n} - \frac{1}{(1-\delta) 2^n} \ge 0$~~

$$G(x) = \frac{\frac{1}{2^n} - \delta \Pr[H=x]}{1-\delta} \ge \frac{\frac{1}{2^n} - \frac{\delta}{\delta 2^n}}{1-\delta} \ge 0. \quad \text{and}$$

$$\sum_{x\in\Sigma^n} G(x) = \frac{\sum_{x\in\Sigma^n}\frac{1}{2^n} - \delta \sum_{x\in\Sigma^n}\Pr[H=x]}{1-\delta} = \frac{1-\delta}{1-\delta} = 1.$$

The mixture distribution is the uniform distribution:

$$\tfrac{1}{2^n} = \Pr[U=x] = \delta \cdot \Pr[H=x] + (1-\delta)\Pr[G=x]$$

$$= \delta \Pr[H=x] + \tfrac{1}{2^n} - \delta \Pr[H=x]$$

$$= \tfrac{1}{2^n}.$$

Thus

$$U_n = \delta H + (1-\delta) G.$$

Pick 2 independent strings uniformly at random. Then

$$U_n^2 = \delta^2 H^2 + (1-\delta)\delta\, GH + \delta(1-\delta)\, HG + (1-\delta)^2 G^2.$$

[Note: HG may not be GH: The notation GH, for example, means that the first string is chosen randomly according to G, and the second, independently, according to H]

Let, for every distribution $\underset{\sim}{D}$ over Σ^n, $P_{\underset{\sim}{D}} = \Pr[C(x_1, x_2) = f(x_1) \oplus f(x_2) \mid x \sim \underset{\sim}{D}]$

assumption: TYAO$_2$

$$\tfrac{1}{2} + \varepsilon \le P_{(U_n)^2} = \delta^2 P_{H^2} + (1-\delta)\delta P_{GH} + \delta(1-\delta) P_{HG} + (1-\delta)^2 P_{G^2}$$

$\frac{\varepsilon}{2} > (1-\delta)^2$ and $P_G^2 \le 1$. Thus $(1-\delta)^2 P_{G^2} \le \frac{\varepsilon}{2}$. Hence

~~$\frac{1}{2} + \frac{\varepsilon}{2} \le (1-\delta)\delta P_{GH} + \delta(1-\delta) P_{HG} + \delta^2 P_{H^2}$~~

$$\tfrac{1}{2} + \tfrac{\varepsilon}{2} \le \delta^2 P_{H^2} + (1-\delta)\delta\, P_{GH} + \delta(1-\delta)\, P_{HG}.$$

Nice

Since $(1-\delta)\delta + \delta(1-\delta) + \delta^2 < 1$, at least one of the probabilities on RHS must be $\geq \frac{1}{2} + \frac{\varepsilon}{2}$

Assume $P_{HG} \geq \frac{1}{2} + \frac{\varepsilon}{2}$.

$$\Pr\left[C(x_1, x_2) = f(x_1) \oplus f(x_2) \mid x_1 \sim H, x_2 \sim G \right] > \frac{1}{2} + \frac{\varepsilon}{2}.$$

By the averaging principle, $\exists$ x_2 such that

$$\Pr_{x \sim H_1}\left[C(x_1, x_2) = f(x_1) \oplus f(x_2) \right] > \frac{1}{2} + \frac{\varepsilon}{2}.$$

$$\Leftrightarrow \Pr_{x \sim H_1}\left[C(x_1, x_2) \oplus f(x_2) = f(x_1) \right] > \frac{1}{2} + \frac{\varepsilon}{2}.$$

This means that we have an S' circuit D (compute $C(x_1, x_2)$ and then XOR with the hardcoded bit $f(x_2)$).

This says that H is not hard wrt. This proves the result for $f^{\oplus}$

Inductively, on k, we can prove this for $(x_1, x_2, \ldots, x_k)$ and $f^{\oplus k}$ □.

Proof of Impagliazzo's Hardcore Lemma.

Proof overview:
This proof, from Arora Barak is non-constructive : shows minmax theorem in probabilistic gametheory ⇒ IHL

Proof

Let $f : \Sigma^n \to \Sigma$ be such that $H_{(f)}^{1-\delta} \geq (s)$ and let $\varepsilon > 0$.

We need a δ-density function H s.t. $\forall C$ of size $\leq \frac{\varepsilon^2 s}{100n}$

cannot compute f only with probability $< \frac{1}{2} + \varepsilon$.

Two player game: Opt: wants to compute f
Pess: wants Opt to fail.

Pess: choose δ-density distribution H
Opt: choose C of size $\leq \frac{\varepsilon^2 s}{100n}$.

Goal of game: at the end, Pess pays Opt ν dollars, $\nu \triangleq \Pr_{x \sim H} [C(x) = f(x)]$

	Opt	Pess
original money	1	1
final money	$1+\nu$	$1-\nu$

This is a 0-sum game, since Pess's loss = Opt's gain.

(Pretty wild connection) Von Neumann min max theorem for 0 sum games states that for whatever value Opt can attain in this game (playing second), if we can adopt randomized strategies, Opt can attain the same value even playing first.

We now consider a randomized game:

- Pess can choose a δ dense distribution at random. [connection with $\delta 2^n$ flat distrns. Exercise]
- Opt can choose a circuit of size $\frac{\varepsilon^2 s}{100n}$ at random.

We have a statement of the form

$$\forall H \quad \exists C \qquad \Pr_{x \sim H} [C(x) = f(x)] \geq \tfrac{1}{2} + \varepsilon. \qquad -(1)$$

[Consider the randomized version.

$$\forall \text{ rand } \delta\text{-density } H \qquad \exists \text{ rand } C \qquad \Pr_{\boxed{C\sim};\, x\sim H} [C(x) = f(x)] \geq \tfrac{1}{2} + \varepsilon \qquad -(2)$$

By the von Neumann minimax theorem,

$$\exists \text{ rand } C \qquad \forall \text{ rand } \delta\text{-density } H \qquad \Pr_{\boxed{C\sim},\, x\sim H} [C(x) = f(x)] \geq \tfrac{1}{2} + \varepsilon \qquad -(3)$$

(same as $\forall H$)

(We need to show $\exists C \quad \forall H \quad \Pr_{x\sim H} [C(x) = f(x)] \geq 1/2 + \varepsilon$)

Call a string x "bad" if $\Pr_{C\sim} [C(x) = f(x)] < 1/2 + \varepsilon$ [Note: The string is fixed, and we randomize over circuits] and "good" otherwise.

Since H is δ-dense, there are at most $\delta \cdot 2^n$ bad strings. (Otherwise we violate (3).)

Choose $C_1, C_2, \ldots, C_t$ ($t = \frac{50n}{\varepsilon^2}$) circuits of size $\frac{\varepsilon^2 S}{100n}$ at random, independent of each other.

Design the circuit C:

$$C(x) \triangleq \text{maj}\{C_1(x), \ldots, C_t(x)\}. \qquad \text{size}(C) \approx \frac{\varepsilon^2 S}{100n} \times \frac{50n}{\varepsilon^2} = \frac{S}{2} < S.$$

Then by Chernoff bound, for every good string x

$$\Pr_{C\sim} [C(x) \neq f(x)] < \frac{1}{2^n}.$$

Hence summing over all good strings,

$$\sum_{x \text{ good}} \Pr_{C\sim} [C(x) \neq f(x)] < 1 \qquad \Rightarrow \exists C \ \forall \text{ good strings},$$