Hardness amplification

Theorem (Impagliazzo-Wigderson '97; STV'99): Let $f \in \mathbb{E}$ be s.t. $H_{wrs}(f) \geqslant S(n)$ for some $S: \mathbb{N} \to \mathbb{N}$. Then $\exists\, g \in \mathbb{E}$, $c \in \mathbb{R}_{>0}$ s.t. $H_{avg}(f) \geqslant S(n/c)^{1/c}$ for all sufficiently large n.

Proof:

- For large n, consider the $tt(f|_{\{0,1\}^n}) =: f_n \in \{0,1\}^N$, $N := 2^n$.
- Encode f_n to $g_{n'} = \text{WH} \circ \text{RM}(f_n) \in \{0,1\}^{N'}$, where $N' = 2^{n'} = 2^{O(n)} = poly(N)$.

  We will take $\underline{n' = 5n}$ & see $g_{n'}$ as the truth-table of a function g on $\{0,1\}^{n'}$.

▷ Since $f \in \mathbb{E}$ & $g_{n'}$ is a $2^{n'}$-length string, we deduce that $g \in \mathbb{E}$.

- Parameters of RM: Fix a small $\delta \in \mathbb{R}_{>0}$.

Assume $n^2 \leq q \leq N$ $\rightarrow$ $q = |\mathbb{F}| = S(n)^\delta =: S^\delta$, $d = \sqrt{q}$, $\ell = \log_d N^2$.

$\Rightarrow$ RM-codeword length is $\binom{d+\ell}{\ell} \geqslant \left(1+\frac{d}{\ell}\right)^\ell \geqslant N$.

⇒ WH∘RM can encode f_n.

• Also, $N' = 2^{n'} = q^{\ell} \cdot q \leq N^4 \cdot N = N^5 = 2^{5n}$.

• Local list decoder: Let us use an lld for WH handling $\left(\frac{1}{2} - S^{-\delta/9}\right)$ errors & an lld for RM handling $\left(1 - 10 \cdot \sqrt{d/q}\right)$ errors.

⇒ lld for WH∘RM handles errors

$$\left(\frac{1}{2} - S^{-\delta/9}\right) \cdot \left(1 - 10 \cdot S^{-\delta/4} \cdot \frac{1}{2 \cdot \left(S^{-\delta/9}\right)^2}\right)$$

$$\geq \left(\frac{1}{2} - S^{-\delta/9}\right) \cdot \left(1 - \frac{5}{S^{\delta/36}}\right) \geq \frac{1}{2} - S^{-\delta/10}.$$

• List-size $= O\left(\left(S^{\delta/9}\right)^2 \cdot \sqrt{q/d}\right) = O(\sqrt{q}) = O(\sqrt{N})$.

• If $\exists$ circuit $G_{n'} \in \mathrm{size}\left(S(n)^{\delta/10}\right)$ computing g on $\frac{1}{2} + S^{-\delta/10}$ of the inputs in $\{0,1\}^{n'}$, then $(\text{WH∘RM-lld}) \circ G_{n'}$, with advice hardwired, yields a circuit of size $S^{c\delta} \cdot S^{\delta/10}$ computing f on $\{0,1\}^n$.

Say, q^c is the complexity of WH∘RM

⇒ $\delta < (c + 0.1)^{-1}$ gives a contradiction.

⇒ $g|_{\{0,1\}^{n'}}$ is $S(n'/5)^{\delta/10}$ - average-case hard. □