Theorem (Impagliazzo, Kabanets, Wigderson 2001):

$$\mathsf{NEXP} \subseteq \mathsf{P/poly} \Rightarrow \mathsf{NEXP} = \mathsf{EXP}.$$

Proof sketch:

- Let us assume that $\mathsf{EXP} \subsetneq \mathsf{NEXP} \subseteq \mathsf{P/poly}$.
- We will derive a contradiction to the time-hierarchy theorem.
- Idea – $\exists L \in \mathsf{NEXP} \setminus \mathsf{EXP}$, which can be used to get a "hard" function. By the "worst-case vs. prg" we get a poly-stretch prg that can "derandomize" $\mathsf{EXP} \subseteq \mathsf{MA}$.

- Pick an $L \in \mathsf{NEXP} \setminus \mathsf{EXP}$. $\exists c > 0$ & a relation $R(x, y)$ testable in $\exp(|x|^{10c})$-time s.t.

$$x \in L \text{ iff } \exists y \in \{0,1\}^{\exp(|x|^c)},\ R(x,y) = 1.$$

- We now consider the complexity of y given x.
- For $D > 0$, let M_D be the following machine:

  On input $x \in \{0,1\}^n$,

1) enumerate boolean circuits of size n^{100D} that

take n^c-bit input & output 1-bit.

2) For each such circuit C, let $tt(C)$ be the 2^{n^c}-long string that corresponds to the truth-table of C.

3) If $\exists$ such C, $R(x, tt(C))=1$ then OUTPUT 1.

4) Else OUTPUT 0.

▷ M_D runs in time $\exp(n^{101D}+n^{10c})$.

• $\because L \notin EXP$, M_D cannot solve L. Thus, $\forall D$, $\exists$ infinite sequence of inputs $X_D := \{s_i \mid i\}$ on which $M_D(s_i)=0$ even though $s_i \in L$.

$\Rightarrow$ $\forall x \in X_D$, the y, for which $R(x,y)=1$, represents the truth-table of a "hard" function that cannot be computed in $Size(n^{100D})$.

• By worst-case-hardness based prg, we can use y to get a ℓ^D-prg G_D.

- We know that $EXP \subseteq P/poly \Rightarrow EXP \subseteq MA$.
- Thus, $\forall L' \in EXP$, Merlin proves $x' \in L'$ by sending a proof, which Arthur can verify by a randomized algorithm in, say, n^D steps ($n := |x'|$).
- Here, Arthur can use the prg G_D.

Let $x'' \in X_D$, $|x''| =: n$. Arthur guesses a string $y \in \{0,1\}^{\exp(n^c)}$ s.t. $R(x'', y) = 1$ & uses y to design G_D.

Using G_D, Arthur reduces the random n^D-bits to n-bits.

this saves us from testing $x'' \in X_D$

▷ Arthur needs $\mathrm{poly}(n^D) \cdot 2^{n^{10c}}$-time, n random bits, n advice bits (for x''), 2^{n^c}-bit guess (for y).

$\Rightarrow \exists c' > 0$ s.t.

▷ $EXP \subseteq \underbrace{\text{i.o.}}_{\text{infinitely-often}}-\mathrm{Ntime}(2^{n^{c'}}) / \underbrace{2n}_{\text{advice-bits}}$.

[For a class $\mathcal{C}$, $L \in \text{i.o.-}\mathcal{C}$ if $\exists M \in \mathcal{C}$ s.t. $L \cap \{0,1\}^n = M \cap \{0,1\}^n$ for ∞-ly many n.]

- $\because$ NEXP $\subseteq$ P/poly, we can further write:
$\exists c'' > 0$, EXP $\subseteq$ i.o.-Size$(n^{c''})$.

- By standard diagonalization this can be ruled out. (Exercise.)

- This contradiction means:
$$\text{NEXP} \neq \text{EXP} \Rightarrow \text{NEXP} \not\subseteq \text{P/poly}. \quad \square$$

— This leads to the result:

<u>Theorem</u> (Impagliazzo & Kabanets, 2003):
$$\text{PIT} \in \text{P} \Rightarrow \text{NEXP} \not\subseteq \text{P/poly} \text{ or } \text{per} \notin \text{AlgP/poly}.$$

Hardness Amplification

- Our goal is to construct average-case hard functions using a function f that is only worst-case hard.

- Idea: View f as a 2^n-length string & apply a map φ that is a "very good" error-correcting code.

Definition: • For $x, y \in \{0,1\}^m$, the fractional Hamming distance $\Delta(x,y) := \frac{\#\{i \mid x_i \neq y_i\}}{m}$.

• For $\delta \in (0,1)$, a function $E : \{0,1\}^n \to \{0,1\}^m$ is an error-correcting code (ECC) with distance δ, if $\forall x \neq y \in \{0,1\}^n$,

$$\Delta(E(x), E(y)) \geqslant \delta .$$

• We call $Im(E) := \{E(x) \mid x \in \{0,1\}^n\}$ the set of codewords.

- These have vast applications.
  In the real world they are used in physical communication channels & the storage media.

- For hardness amplification:
  Let f be a worst-case hard boolean function. Let f' be the $N = 2^n$-bit string expressing $tt(f)$.
  We encode f' by an ECC $E : \{0,1\}^N \to \{0,1\}^{N^c}$. Thus, $E(f')$ is a 2^{cn}-bit string expressing $tt(g)$, for some $g : \{0,1\}^{cn} \to \{0,1\}$.
  We will show that if E with nice local decoding properties exists then g is an average-case hard function.
  (Also, $f \in \mathbb{E} \Rightarrow g \in \mathbb{E}$.)