A decidable language that is not in $\mathbf{P}$

Vassos Hadzilacos

**Theorem 7.2** The language

$$EXP = \{(M, x) : M \text{ accepts } x \text{ in at most } 2^{|x|} \text{ steps}\}$$

is decidable but it is not in $\mathbf{P}$.

**Proof.** To decide whether $\langle M, x \rangle \in EXP$, we run the universal Turing machine on input $\langle M, x \rangle$ for up to $2^{|x|}$ steps or until $M$ on $x$ halts, whichever happens first. If $M$ accepts $x$ within that number of steps, we accept; otherwise we reject.

To prove that $EXP \notin \mathbf{P}$ we use a form of diagonalization. Suppose, for contradiction, that $EXP \in \mathbf{P}$. Then the language

$$EXP' = \{\langle M \rangle : M \text{ accepts } \langle M \rangle \text{ in at most } 2^{|\langle M \rangle|} \text{ steps}\}$$

is also in $\mathbf{P}$. (This is because, from input $\langle M \rangle$ we can first construct $\langle M, \langle M \rangle \rangle$ in polytime, and then use this as input to a polytime Turing machine $M_{EXP}$ that decides $EXP$; the answer of $M_{EXP}$ on $\langle M, \langle M \rangle \rangle$ tells us whether $\langle M \rangle \in EXP'$.)

Now consider the complement of $EXP'$, which we denote $D$ (for “diagonal”):

$$D = \{\langle M \rangle : M \text{ does not accept } \langle M \rangle \text{ in at most } 2^{|\langle M \rangle|} \text{ steps}\}.$$ 

Since $EXP'$ is in $\mathbf{P}$, so is its complement $D$. (All we have to do is negate the output of a polytime Turing machine that decides $EXP'$.) So, let $M_D$ be a polytime Turing machine that decides $D$, and let $p(n)$ be a polynomial that is an upper bound on the running time of $M_D$. Because $p(n)$ is a polynomial, there is some natural number $n_0$ such that for all $n \geq n_0$, $p(n) \leq 2^n$. (This is because every polynomial $n^k$, no matter how large the degree $k$, is eventually dominated by every exponential $b^n$, no matter how small the base $b > 1$.) Without loss of generality, we can assume that $|\langle M_D \rangle| \geq n_0$. (This is because we can pad $M_D$ with junk states or tape symbols — i.e., states that $M_D$ never enters or tape symbols that it never writes — to make its description longer than $n_0$.) So,

$$p(|\langle M_D \rangle|) \leq 2^{|\langle M_D \rangle|}. \quad (*)$$

Now let’s see what happens if we unleash $M_D$ on itself. There are two cases.

**Case 1.** $M_D$ accepts $\langle M_D \rangle$. Since the running time of $M_D$ is bounded from above by the polynomial $p(n)$, we have that $M_D$ accepts $\langle M_D \rangle$ in at most $p(|\langle M_D \rangle|)$ steps. By $(*)$, $M_D$ accepts $\langle M_D \rangle$ in at most $2^{|\langle M_D \rangle|}$ steps. Thus, by the definition of $D$, $\langle M_D \rangle \notin D$; and since $M_D$ is a decider for $D$, $M_D$ does not accept $\langle M_D \rangle$, contrary to the hypothesis of Case 1.

**Case 2.** $M_D$ does not accept $\langle M_D \rangle$. In particular, $M_D$ does not accept $\langle M_D \rangle$ in at most $2^{|\langle M_D \rangle|}$ steps. By definition of $D$ then, $\langle M_D \rangle \notin D$; and since $M_D$ is a decider for $D$, $M_D$ accepts $\langle M_D \rangle$, contrary to the hypothesis of Case 2.

Since both cases lead to contradiction, our original assumption, that $EXP \in \mathbf{P}$, is false. Therefore $EXP \notin \mathbf{P}$, as wanted. \qed