A decidable language that is not in **P**

Vassos Hadzilacos

Theorem 7.2 *The language*

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

is decidable but it is not in ***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 **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"):

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

Since EXP' is in **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 n^k be a polynomial that is an upper bound on the running time of M_D. Then there is some natural number n_0 such that for all $n \geq n_0$, $n^k \leq 2^n$. (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, $|\langle M_D\rangle|^k \leq 2^{|\langle M_D\rangle|}$. Therefore

$$M_D \text{ on input } \langle M_D\rangle \text{ halts (accepts or rejects) in at most } 2^{|\langle M_D\rangle|} \text{ steps.}$$

Now let's see what happens if we unleash M_D on its own code. There are two cases.

Case 1. M_D accepts $\langle M_D\rangle$ (in at most $2^{|\langle M_D\rangle|}$ steps). Since M_D decides D, this means that $\langle M_D\rangle \in D$ and, by definition of D, this implies that M_D does not accept $\langle M_D\rangle$ in at most $2^{|\langle M_D\rangle|}$ steps, contrary to the hypothesis of Case 1.

Case 2. M_D rejects $\langle M_D\rangle$ (in at most $2^{|\langle M_D\rangle|}$ steps). Then $\langle M_D\rangle \notin D$, and so M_D accepts $\langle M_D\rangle$ in at most $2^{|\langle M_D\rangle|}$ steps, 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. $\square$