A PROOF OF $\mathrm{P} \neq \mathrm{NP}$

VICTOR PORTON

ABSTRACT. My proof that $\mathrm{P} \neq \mathrm{NP}$.

I denote $s(X)$ the size of data X (in bits).

Assume $\mathrm{P} = \mathrm{NP}$.

Fix some formal system such as ZF.

I will call a statement X *coherent* when there is a proof of X or $\neg X$.

I will call a set coherent when each its member is coherent (recursively by the axiom of foundation).

Let E be the set of set definitions X such that there is no polynomial-size (regarding $s(X)$) proof of coherence of X.

Let M be the set defined by the set-definition

$$\{\text{set definition } X \text{ with polynomial-size proof of coherence} \mid X \notin E\}.$$

M has polynomial-size proof of coherence, because $X \notin E$ means X has polynomial-size $p(s(X))$ proof of coherence, what can be proved by checking $2^{p(s(X))}$ variants (that's a P problem in our assumption, therefore the proof of the existence of the proof is polynomial-size) of every X. (That may not work for small $s(X)$, but small cases can be checked individually in constant time.)

Therefore:

$$M \in E \Leftrightarrow M \notin E.$$

Contradiction.

$\mathrm{P} \neq \mathrm{NP}$.

Email address: `porton@narod.ru`