A PROOF OF P $\neq$ NP

VICTOR PORTON

ABSTRACT. My proof that P $\neq$ NP.

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

Whether there is or there is no at-most w-size proof of a statement X are two NP-problems, because it can be non-deterministically verified in polynomial time using the merkle tree of execution of a proof-checking algorithm (like as in Cartesi crypto).

Assume P = NP.

Then whether there is a w-size proof of a statement X is an NP and therefore P problem.

Fix some formal system such as ZF.

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

Let E be the set of set definitions X such that members of X have polynomial-size (regarding $s(X)$) proofs of coherence of X.

Let M be the set defined by the set-definition

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

M has polynomial-size proofs of coherence, because $X \notin E(X)$ means X is not having polynomial-size proofs of coherence, what can be proved by checking that there exists a proof of "X has no polynomial-size proofs of coherence" with the maximum length $2^{s(X)}$ (that's a P problem in our assumption, therefore the proof of the existence of the proof is polynomial-size) of every X. (That fails for small sizes of X, but they can be solved individually in constant size.)

Therefore:

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

Contradiction.

P $\neq$ NP.

Email address: porton@narod.ru