Consequences of NP=PSPACE

What would be the nasty consequences of NP=PSPACE? I am surprised I did not found anything on this, given that these classes are among the most famous ones.

In particular, would it have any consequences on the lower classes?

cc.complexity-theory complexity-classes conditional-results

edited Feb 14 '14 at 10:52 András Salamon 13.1k 3 47 127

asked Feb 13 '14 at 17:11 Denis 4,079 14 34

4 An immediate corollary, or rather a reformulation of the identity: the verifier wouldn't need to message back the prover, ever! – Alessandro Cosentino Feb 13 '14 at 23:44

4 Answers

If $\mathsf{NP} = \mathsf{PSPACE}$, this would imply:

- $\mathsf{P}^{\#\mathsf{P}} = \mathsf{NP}$
  That is, counting the solutions to a problem in NP would be polytime reducible to finding a single solution;
- $\mathsf{PP} = \mathsf{NP}$
  That is, polynomial-time randomized algorithms with success probability arbitrarily close to 1/2 is polynomial-time reducible to polynomial-time randomized algorithms with one-sided error, where YES instances are accepted with arbitrarily small probability;
- $\mathsf{MA} = \mathsf{NP}$
  That is, for any problem which is verifiable in polynomial time, randomization provides a polynomial-time speedup at best (but this is just a corollary of the polynomial-time hierarchy collapsing);
- $\mathsf{BQP} \subseteq \mathsf{NP}$
  That is, any problem which is solvable by a quantum computer has easily verified certificates for its answers; this would be an important positive result in the philosophy of quantum mechanics, and would probably be helpful to the effort to construct quantum computers (for verifying that they are doing what they are meant to be doing).

All of these are due to containments of the classes on the left-hand sides in PSPACE (though we also have $\mathsf{BQP} \subseteq \mathsf{PP}$).

edited Feb 14 '14 at 0:46

answered Feb 13 '14 at 20:02 Niel de Beaudrap 6,656 21 62

Can you point to a reference where $\mathbf{NP} = \mathbf{PSPACE}$ implies that $\mathbf{BQP} \subseteq \mathbf{NP}$. Thanks – Qui s'en soucie Feb 13 '14 at 22:23

2 @TayfunPay You basically want a reference for $\mathsf{BQP} \subseteq \mathsf{PSPACE}$. The reference for that is BV97. However, you can also prove that $\mathsf{BQP} \subseteq \mathsf{PP}$. See the following lecture for intuition on this: scottaaronson.com/democritus/lec10.html – Alessandro Cosentino Feb 13 '14 at 23:24

1 @AlessandroCosentino Yes, I knew that $\mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PP} \subseteq \mathbf{PSPACE}$ and that $\mathbf{NP} \subseteq \mathbf{PP} \subseteq \mathbf{PSPACE}$. I guess I just needed to be pointed out to jiggle my memory! Thanks! :) – Qui s'en soucie Feb 13 '14 at 23:58

If $\mathbf{NP} = \mathbf{PSPACE}$

1) Polynomial Hierarchy would collapse to $\mathbf{NP}$.

2) We will now have that $\mathbf{NP} \neq \mathbf{NL}$ since we know that $\mathbf{PSPACE} \neq \mathbf{NL}$

---UPDATE---

3) It is known that $\mathbf{NL} \subseteq \mathbf{C_{=}L} \subseteq \mathbf{PL}$, where they are the logarithmic space bounded versions of $\mathbf{NP}$, $\mathbf{C_{=}P}$ and $\mathbf{PP}$ respectively. Then by definition none of these complexity classes could be equal $\mathbf{NP}$ under the assumption that $\mathbf{NP} = \mathbf{PSPACE}$.

edited Feb 14 '14 at 1:49

answered Feb 13 '14 at 19:28 Qui s'en soucie 1,065 2 9 33

1 These are trivial consequences following PH⊆PSPACE and NL≠PSPACE, I was hoping for more surprising consequences, for instance something between NL and P, or any new relation between two classes "strictly" below NP. – Denis Feb 13 '14 at 19:44

1 Note that if you consider **NL** as the class of languages which have solutions which can be verified in logspace, *even if each symbol of the solution is read at most once* (albeit where logarithmically many can be stored on the work tape at any one time), the fact that it differs from **NP** indicates that there is a class **L'** which is a relative of **L**, involving Turing Machines with two input tapes but where one is read-once and the other is not, and which is different from **P** (where because one has polynomial space on the worktape, read-once input limitations don't matter). – Niel de Beaudrap Feb 13 '14 at 20:25

@dkuper You would also have $\mathbf{PL} \neq \mathbf{NP}$, where $\mathbf{PL}$ is the logarithmic space bounded version of $\mathbf{PP}$ as well as $\mathbf{\#L} \neq \mathbf{NP}$, where $\mathbf{\#L}$ is the logarithmic space bounded version of $\mathbf{\#P}$. – Qui s'en soucie Feb 13 '14 at 22:15

1 @dkuper see math.ucdavis.edu/~greg/zoology/diagram.xml – Qui s'en soucie Feb 13 '14 at 22:19

1 @TayfunPay: (1) why don't you edit your answer to include the relationships from your comment? (2) How do they hold? – Niel de Beaudrap Feb 14 '14 at 0:45

|

One point which has been implicitly but not explicitly mentioned yet is that we would get $\mathsf{NP} = \mathsf{coNP}$. Although this is equivalent to PH collapsing to NP, it follows directly from the fact that PSPACE is closed under complement, which is trivial to prove.

I think $\mathsf{NP} = \mathsf{coNP}$ is worth pointing out on its own because of the large number of surprising consequences it has: there are short proofs witnessing when a graph is *not* 3-colorable, *non-*Hamiltonian, when two graphs are *non-*isomorphic, ..., and (in some sense more generally) that there is some Cook-Reckhow proof system in which *every* propositional tautology has a polynomial-sized proof.

answered Feb 14 '14 at 1:06
Joshua Grochow
26.6k 3 89 171

In addition to the results pointed in all other answers, there is a one involving Interactive Proof Systems ($\mathbf{IP}$), that are the generalization $\mathbf{NP}$ where Verifier and Prover exchange messages in order to recognize a language.

It is known that $\mathbf{IP} = \mathbf{PSPACE}$, so if $\mathbf{NP} = \mathbf{PSPACE}$, it means that only one message is sufficient! For me the more impressing of this result is that the Verifier wouldn't need to challenge the Prover and can trust the very first message sent by her.

edited Feb 14 '14 at 20:20

answered Feb 14 '14 at 2:01
Alex Grilo
267 1 8

It could still depend on the implementation though? Meaning there would still be interactive provers needing more exchangse, only there exists others with only one message for the same language. – Denis Feb 14 '14 at 10:10

Well, it would mean that one message is sufficient. If I understood your question correctly, it's the same for problems in P: although there are polynomial time algorithms for them, one can still create an exponential time algorithm. – Alex Grilo Feb 14 '14 at 10:38

2 @AlexGrilo: hence my comment under the question :) – Alessandro Cosentino Feb 14 '14 at 13:54

@AlessandroCosentino Sorry, I didn't see it before – Alex Grilo Feb 14 '14 at 14:43