Review of: "SAT is as hard as solving Homogeneous Diophantine Equation of Degree Two"

Leo Liberti[1]

1 Ecole Polytechnique

Potential competing interests: No potential competing interests to declare.

The reduction exhibited in the paper seems valid to me – it rests on the observation that

x XOR y = |x - y| = (x - y)^2

whenever x,y in {0,1}.

I have not checked whether this observation is original. It's one of those easy observations that might be made all the time, yet never written down as a publication by itself. I'm not adverse to publishing this just on the account of the simplicity of the proof – quite on the contrary, I think it might be useful as a link between the simple observation above, and the consequence given in the title of this paper. Speaking of which, don't you rather mean that Homogeneous Diophantine Equations of Degree Two are as hard as SAT, rather than the reverse? You are reducing a variant of SAT to HDE2, after all, which means that HDE2 cannot be easier than SAT, implying that HDE2 is at least as hard as SAT.

I might advise a revision along these lines: you made no use of the two constants B, M. For what values of B, M is the HDE2 problem hard? Or polytime? Can you make further contributions along these lines in order to enrich your paper?