On the Quantitative Hardness of CVP

Noah Stephens-Davidowitz
Princeton University

9/27/2017 at 11:00 am
CoRE A 301

Abstract

For odd integers $p \geq 1$ (and $p = \infty$), we show that the Closest Vector Problem in the $\ell_p$ norm (CVP$_p$) over rank $n$ lattices cannot be solved in $2^\{(1-\epsilon)n\}$ time for any constant $\epsilon > 0$ unless the Strong Exponential Time Hypothesis (SETH) fails. We then extend this result to “almost all” values of $p \geq 1$, not including the even integers. This comes tantalizingly close to settling the quantitative time complexity of the important special case of CVP$_2$ (i.e., CVP in the Euclidean norm), for which a $2^\{n + o(n)\}$-time algorithm is known.

We also show a similar SETH-hardness result for SVP$_\infty$; hardness of approximating CVP$_p$ to within some constant factor under the so-called Gap-ETH assumption; and other hardness results for CVP$_p$ and CVPP$_p$ for any $1 \leq p < \infty$ under different assumptions.