

# A Framework of Quantum Strong Exponential-Time Hypotheses



Harry Buhrman, Subhasree Patro, Florian Speelman  
QuSoft, CWI and University of Amsterdam



Heard of the SATISFIABILITY (SAT) problem?

Umm, no!

Given a Boolean formula with  $n$  variables, is there a satisfying assignment to these  $n$  variables?

Fun fact: Best known algorithm for SAT takes  $2^n$  classical time, while the best known lower bound is  $n$ .

In 2001, Impagliazzo, Zane and Paturi conjectured that SAT requires  $2^n$  time.

They called it the Strong Exponential-Time Hypothesis (SETH).

Was SETH useful?

Yes! It was useful in proving conditional lower bounds for many problems.

For example: In 2005, R. Williams used SETH to prove quadratic lower bound for Orthogonal Vectors (OV) problem.

Thereafter, OV was used to prove tight quadratic lower bounds for string problems like Edit Distance, Longest Common Subsequence (LCS), etc.

Wait! Does SETH hold relative to quantum computation?

No! Using Grover's subroutine SAT can be solved in  $2^{n/2}$  quantum time.

In 2019, we and Aaronson et al. conjectured that SAT requires  $2^{n/2}$  quantum time.

We called it the Basic-QSETH.

What happens to the SETH based lower bounds in the quantum setting?

For most problems,  $T$  SETH-based lower bound becomes  $\sqrt{T}$  conditioned on Basic-QSETH.

Not all of them remain tight. While the Basic-QSETH based linear lower bound for OV is tight, it isn't for Edit Distance and LCS.

We give a workaround.

We notice that variants of SAT like Parity-SAT might not be amenable to Grover like speedup.

It is believable that Parity-SAT requires  $2^n$  on a quantum computer: Parity-QSETH.

Right! Because the query complexity of properties like PARITY is maximum.

Almost! PARITY has high query complexity in general, but it only has to be computed on truth table of small formulas.

In fact, it is shown by Ambainis et al. and Robin Kothari et al. that any property can be computed in  $2^{n/2} \log |S|$  queries. Here  $S$  is the set of strings.

We give another workaround.

We introduce the notion of Compression Oblivious properties.

Compression Oblivious properties: Time taken to compute these properties on a small set of strings is at least the query complexity of these properties on all strings.

We conjecture that for all compression oblivious properties computing these on Boolean formulas is lower bounded by the query complexity of these properties on all strings: The QSETH conjecture.

How is that going to help?

Parity-QSETH implies PARITY is compression oblivious, which means The Proofs of Useful Work scheme by Ball et al. holds in the quantum setting under our QSETH conjecture.

Additionally, we observe that the reductions from SAT to Edit Distance (and LCS) by Abboud et al. compute a more complicated property on the truth table of the Boolean formula. We call the property  $P_{edit}$  (and  $P_{lcs}$ ).

We show that  $P_{edit}$  has a query complexity of  $2^{0.75n}$  on all strings of length  $2^n$ .

Assuming,  $P_{edit}$  is compression oblivious and assuming our QSETH conjecture, we show that Edit Distance requires  $n^{1/2}$  quantum time.

Why are you assuming  $P_{edit}$  or PARITY are compression oblivious, can't you prove it?

Umm, not yet. If we can prove that properties like these are compression oblivious then we can separate P from PSPACE.

Interesting, a proof barrier!

What's next then?

We could use our QSETH framework to give conditional lower bounds for other problems in BQP.

Notion of compression obliviousness seem interesting to study independently as well.

We could study other key problems like 3SUM and APSP in the quantum setting that have been used in classical setting to prove lower bounds for many problems.

Thanks!