Algorithmic Lower Bounds - Exponential Time Hypothesis

Matt Kovacs-Deak

December 11, 2021

A series of results established running time lower bounds for solving 3-SAT in terms of the number of variables n. For example, (i) Makino *et al.* obtained an $O(1.3303^n)$ deterministic algorithm, (ii) Hertli obtained an $O(1.308^n)$ randomized algorithm. More generally, for $k-SAT$ (iii) Dantsin *et al.* obtained a deterministic $O((2-\frac{1}{k+1})^n)$ deterministic algorithm and Paturi *et al.* obtained an $O(2^{n-n/k})$ randomized algorithm.

While these results might be improved in the future, it is believed that 3-SAT requires $2^{\Omega(n)}$ time. This belief is captured by the *Exponential Time Hypothesis* formulated by Impagliazzo and Paturi: For any $k \in \mathbb{Z}^+$ let $s_k = \inf\{s : \text{ an } O(2^{sn}) \text{ algorithm exists for k-SAT }\}$.

Conjecture 1 (Exponential Time Hypothesis)**.** *For all $k \geq 3$, $s_k > 0$.*

Conjecture 2 (Strong Exponential Time Hypothesis)**.** *The sequence (s_k) converges to 1.*

Notice that (1) the ETH implies $\mathbf{P} \neq \mathbf{NP}$, (2) the ETH is equivalent to $s_3 > 0$ as the sequence (s_k) is non-decreasing.

For the above n denoted the number of variables. Impagliazzo *et al.* however proved that one can equivalently formulate the above hypotheses in terms of the actual length of the input formulae. This can be done using the following result,

Lemma 3 (The Sparsification Lemma)**.** *For any $k \in \mathbb{N}$ and $\epsilon > 0$, there is some $c > 0$ and an algorithm $\mathcal{A}$ such that given a k-CNF formula ϕ on n variables:*

(i) $\mathcal{A}$ returns t k-CNF formulas $\phi_1, ...\phi_t$, where $t \leq 2^{\epsilon n}$,

(ii) Each ϕ_i involves at most cn clauses,

(iii) $\phi \in SAT$ iff $\phi_i \in SAT$ for some i,

(iv) $\mathcal{A}$ runs in $O(p(n)2^{\epsilon n})$ time for some polynomial p.

Using the above lemma one can prove that the ETH and the SETH can be equivalently formulated by characterizing the runtimes in terms of the actual input lengths n'.

Assuming that the ETH is true, one can prove lower bounds of many problems. Given some polynomial reduction $A \leq_p B$ via some f, we'll say that the reduction has *linear blowup* if $|f(x)| \in \Theta(|x|)$. Analogously if $|f(x)| \in \Theta(|x|)$, we'll say that the reduction has *quadratic blowup*. Notice that if 3-SAT $\leq_p B$ with a linear blowup then every algorithm that solves B must run in $O(2^{\Omega(n)})$ time. An analogous statement can be made for when the reduction has quadratic blowup. Using the above observation one can leverage many standard reductions to show the following,

Theorem 4. *Assume that the ETH holds. Then each of the following problems require $2^{\Omega(n)}$ time: Vertex Cover, 3-Colorability, Clique, Directed Hamiltonian Cycle. Each of these can be shown using the standard reductions from 3-SAT. Additionally via a reduction from Vertex Cover, the same runtime is required for Dominating Set.*

Reductions that have quadratic blowup can be used to prove that (assuming the ETH) certain problems require $O(2^{\Omega(n)})$ time to solve:

Theorem 5. *Along the standard reductions (from* `3-SAT`*) that have quadratic blowup the following problems all require $O(2^{\Omega(\sqrt{n})})$ time to solve when restricted to planar graphs: 3-colorability, 3-colorability of 4-regular graphs, Dominating Set, Directed Hamiltonian Cycle, Vertex Cover.*

One might wonder if the bounds of the above claim can be improved to $2^{\Omega(n)}$. This question however is already settled (*unconditionally*), and all of the mentioned problems are in $2^{\Omega(\sqrt{n})}$.

Conditional on the ETH one can prove results about *fixed parameter tractability* (FTP). It is known that VC_k can be solved in $O(2^k n)$. Assuming the ETH this bound is tight:

Theorem 6. *Assume the ETH, and let $l \in \mathbb{N}^+$. Then the k-parameterized versions of Vertex Cover, Clique, Dominating Set, and Directed Hamiltonian cycle problems all require $n^l 2^{\Omega(k)}$ time to solve.*

As before, one can prove analogous results for the planar restrictions of the above problems. Clique is an exception, as restricted to planar graphs clique is in **P**.

Theorem 7. *Assuming the ETH, the k-parameterized versions of the planar restrictions of Vertex Cover, Dominating Set, and Directed Hamiltonian cycle all require $n2^{\Omega(\sqrt{k})}$ time to solve.*

Next, we'll show that ETH implies $f(k)n^{\Omega(k)}$ lower bounds for certain problems. Note that it can be shown that there is no function f such that CLIQ_k can be solved in $f(k)n^{O(1)}$ time. The ETH can be used to make to strengthen this statement.

Theorem 8. *Assume the ETH, and let $f(k)$ be any computable function. Then both CLIQ_k and IS_k require $f(k)n^{\Omega(k)}$ time to solve.*

The above result serves as a building block to show additional $f(k)n^{\Omega(k)}$ lower bounds. First we need the following notion.

Definition 9. *Let $\mathcal{A}$ and $\mathcal{B}$ be parameterized problems. A k-linear FPT reduction from $\mathcal{A}$ to $\mathcal{B}$ is an FPT reduction such that whenever (x, k) is mapped to (y, l), $l \in O(k)$.*

Using the above definition one can prove the following:

Claim 10. *Assume the ETH and let f be some computable function.*

(i) Let A_k be some parameterized problem, and assume that CLIQ_k reduces to A_k via a k-linear reduction. Then A_k requires $f(k)n^{\Omega(k)}$ time.

(ii) The k-parameterized versions of each of the following problems require $f(k)n^{Omega(k)}$ time to solve: Independent Set, Dominating Set, Set Cover, and Partial Vertex Cover.

Next we'll define the Grid Tiling problem, which will serve as a building block for deriving lower bounds for some problems (these results are due to Cygan *et al.*). Let $k \in \mathbb{N}^+$, then an instance of the k-Grid Tiling Problem (GRID_k) is a $k \times k$ matrix S such that each entry $S(i, j)$ is a subset of $[n] \times [n]$ for some (given) $n \in \mathbb{N}^+$. The objective of the GRID_k problem is to decide whether there are ordered pairs $(a_i, b_j) \in S(i, j)$ such that both $(a_i, b_j) = (a_{i+1}, b_j)$, and $(a_i, b_j) = (a_i, b_{j+1})$. One can prove that,

Theorem 11. *(i) There is a k-linear FPT reduction from CLIQ_k to GRID_k.*

(ii) Assuming the ETH, for any computable function f, GRID_k *requires* $f(k)n^{\Omega(k)}$ *time to solve.*

The above result allows obtaining lower bounds for the LIST COLORING PROBLEM (LC). Consider a graph $G = (V, E)$, together with a collection of colors $L_v \subset [n]$ for each vertex v of G, where n is the number of colors. The objective of the LC is to determine whether there is a proper coloring $c : V \to [n]$ of G such that $c(v) \in L_c$ for all vertices $v \in V$. The restriction of LC to planar graphs of treewidth k will be denoted $\texttt{PL-LC}_k$.

Theorem 12. *There is a k-linear FPT reduction from* GRID_k *to* $\mathrm{PL\text{-}LC}_k$*.*

We close these notes by defining three problems to which GRID_k can be reduced:

(i) The *k-Grid Tiling LE Problem* ($\texttt{GRIDLE}_k$): given a $\texttt{GRID}_k$ instance S, decide if there are $(a_i, b_j) \in S(i, j)$ such that both $a_i \leq a_{i+1}$ and $b_j \leq b_{j+1}$.

(ii) The *Scattered Set Problem* (SCAT): given a graph G together with two integers k, d, decide if there are k vertices of G with pairwise distance at least d.

(iii) The *Unit Disk Independent Set Problem* (UDIS): given a set $P \in \mathbb{R}^2$ of points in the plane together with some $k \in \mathbb{N}$, decide if there is some subset of k points $P' \subseteq P$ such that $2 < d(p, q)$ for all $p, q \in P'$.

Theorem 13. *(i) There is a k-linear FPT reduction from* $\texttt{GRID}_k$ *to* $\texttt{GRIDLE}_k$*.*

(ii) There is a k-linear FPT reduction from $\texttt{GRIDLE}_k$ *to SCAT.*

(iii) There is a k-linear FPT reduction from $\texttt{GRIDLE}_k$ *to UDIS.*

Further reading

- The ORTHOGONAL VECTORS PROBLEM (OV) is the following: given two sets $A, B \subseteq \{0, 1\}^d$ of equal size, are there $a \in A, b \in B$ with $a \perp b$? Writing $n = |A| = |B|$, notice that OV can be solved straightforwardly in $O(n^2 d)$ time. It is conjectured that one cannot do much better: the *Orthogonal Vectors Hypothesis* (OVH) asserts that there is no algorithm that solves OV in time $O(n^{2-\epsilon}\,\mathrm{poly}(d))$ for any $\epsilon > 0$. Williams [5] showed that the Strong Exponential Time Hypothesis implies the OVH.

- A lattice $\mathcal{L}$ in $\mathbb{R}^n$ is just a discrete subgroup of $\mathbb{R}^n$. The CLOSEST VECTOR PROBLEM (CVP) is: given a *lattice* $\mathcal{L}$ (specified through a basis) together with some target vector $v \in \mathbb{R}^n$ output $u \in \mathcal{L}$ that is closest to v. To indicate that the p-norm is being used, the notation SVP_p has been adopted. Aggarwal *et al.* [1] showed that for $p \notin 2\mathbb{Z}$, $\texttt{CVP}_p$ cannot be solved in time $O(2^{(1-\epsilon)n})$ for any $\epsilon > 0$, assuming the SETH.

- A problem closely related to CVP is the SHORTEST VECTOR PROBLEM (SVP): given a lattice $\mathcal{L}$ output a lattice vector $v \in \mathcal{L}$ of minimal norm. By producing a reduction from CVP to SVP that increases the *rank* of the lattice by a constant multiplicative factor, Aggarwal *et al.* [2] extended the above result to SVP.

- Despite the above results, many open questions remain [3] regarding the *fine-grained* complexity of lattice problems. As an example we state one open question: Is there a $O(2^{0.99n})$ time algorithm for SVP assuming the Strong Exponential Time Hypothesis?

- Finally, we note that despite what the terminology alludes to, the implication SETH $\Rightarrow$ ETH is not straightforward. Nonetheless, the implication is indeed true, and the interested reader can consult Impagliazzo *et al.* [4]. Note, however, that the reverse implication has not been ruled out yet.

References

[1] D. Aggarwal, H. Bennett, A. Golovnev, and N. Stephens-Davidowitz. Fine-grained hardness of CVP(P) - everything that we can prove (and nothing else). *CoRR*, abs/1911.02440, 2019.

[2] D. Aggarwal and N. Stephens-Davidowitz. (gap/s)eth hardness of SVP. *CoRR*, abs/1712.00942, 2017.

[3] H. Bennett, S. Golovnev, and N. Stephens-Davidowitz. Fine-grained hardness of lattice problems: Open questions posted on may 3, 2020 by huck bennett, sasha golovnev and noah stephens-davidowitz. `https://blog.simons.berkeley.edu/2020/05/fine-grained-hardness-of-lattice-problems-open-questions/`.

[4] R. Impagliazzo, R. Paturi, and F. Zane. Which problems have strongly exponential complexity? *Journal of Computer and System Sciences*, 63(4):512–530, 2001.

[5] R. Williams. A new algorithm for optimal 2-constraint satisfaction and its implications. *Theoretical Computer Science*, 348(2):357–365, 2005. Automata, Languages and Programming: Algorithms and Complexity (ICALP-A 2004).