CMSC 858M: Algorithmic Lower Bounds: Fun with Hardness Proofs
Fall 2020

Instructor: Mohammad T. Hajiaghayi
Scribe: Jacob Prinz

December 11, 2021

1 Overview

Many algorithms have been shown to be NP-complete. Most computer scientists believe that $\mathsf{P} \neq \mathsf{NP}$, and that therefore all of these problems have no polynomial time algorithm. However, nobody has found any algorithm for any of these problems which runs in much better than exponential time. This has prompted the Exponential Time Hypothesis, that NP-complete problems take exponential time to run on a deterministic turing machine.

2 Exponential Time Hypothesis

In order to show that $\mathsf{P} \neq \mathsf{NP}$, all that one has to do is show that any problem in NP takes longer than polynomial time to run. However, in reality it is strongly believed that ALL NP-complete problems take exponential time to run. Variations of SAT are often used as an NP complete problem. The following results for algorithms for SAT have been found:

- Makino et al. [?] found a deterministic $O(1.3303^n)$ algorithm for 3SAT
- Hertli [?] found a randomized $O(1.308^n)$ time algorithm for 3SAT
- Dantsin et al. [?] found a $O((2 - \frac{1}{k+1})^n)$ time deterministic algorithm for kSAT.
- Paturi et al. [?] found a $O(2^{n-(n/k)})$ time randomized algorithm for kSAT.

It is believed to be possible that the 3SAT will be solved in $O(\alpha^n)$ for some $1 < \alpha < 1.3$. However, it is conjectured that the runtime will always be

exponential. It is possible for SAT to have runtimes that are very slightly less that exponential.

Definition 1 $s_k = \inf\{s : \textit{ there is an } O(2^{sn}) \textit{ algorithm for } kSAT\}$

All of the algorithms for kSAT mentioned in the bulleted list above have time complexity of the form 2^{cn}. Also, it seems that as k increases, so does c become closer to 1. Impagliazzo and Paturi conjectured the following:

conjecture 1

- *Exponential Time Hypothesis (ETH): For all* $k \geq 3$, $s_k > 0$. *Because* $s_3 \leq s_4 \leq ...$, *this can be stated more simply as* $s_3 > 0$. *This is in turn equivalent to that 3SAT takes* $2^{\Omega(n)}$ *time.*
- *Strong Exponential Time Hypothesis (SETH): The sequence* $s_3, s_4, s_5, s_6, s_7, ...$ *converges to 1.*

n is the number of variables. Suppose instead that we want to classify SAT problems by the length of the input. Impagliazzo et al. [?] towards that end proved this lemma:

Lemma 1 (The Sparsification Lemma) *Let* $k \in N$ *and* $\epsilon > 0$. *Then there exists a constant* c *and an algorithm which does the following:*

- *Inputs a k-CNF formula*
- *Outputs* t *k-CNF formulas* $f_1, ...f_t$ *and* $t \leq 2^{\epsilon n}$, *and each* f_i *has* $\leq cn$ *clauses.*
- $f \in SAT$ *iff there is some* i *such that* $f_i \in SAT$
- *The algorithm runs in time* $O(2^{\epsilon n}p(n))$ *for some polynomial* p.

Exercise: Show that changing ETH so that n is the length of the input rather than the number of clasuses is equivalent to the given statement of ETH.

Note that ETH is much stronger than $P \neq NP$. Therefore, proving the hypothesis is at least as hard as proving that $P \neq NP$. However, it is strongly believed to be true. We will use it as an assumption to prove lower bounds on other problems.

Definition 2 *The blowup of a reduction is the size of the output problem as a function of the size of the input problem.*

Suppose that $A \leq_p B$ *via* f

- f *has a linear blowup if* $|f(x)| \leq O(|x|)$
- f *has quadratic blowup if* $|f(x)| = \Theta(|x|^2)$

Exercise: Derive the following results assuming ETH:

- Suppose that $3SAT \leq_p B_1 \leq_p B_2 \leq_p ... \leq_p B_L$, where each reduction has linear blowup. Show that for each i B_i runs in $2^{\Omega(\sqrt{(n)})}$
- Suppose that $3SAT \leq_p B_1 \leq_p B_2 \leq_p ... \leq_p B_L$. One of the reductions is quadratic, but the rest are linear.
- Would it be possible to derive anything useful if all of the reductions were quadratic?

By assuming that $P \neq NP$, if we can reduce from some NP complete problem to some other problem with polynomial blowup, we can show the other problem is not in P.

If we assume ETH and use a reduction with quadratic blowup, we can get a $O(2^{\Omega(n)})$ time lower bound.

3 $2^{Omega(n)}$ lower bounds from ETH

To show a $2^{\Omega(n)}$ lower bound on a problem, all we need is a reduction from ETH with lienar blowup. Many of these reductions have been done in class, such as

- Linear blowup reduction from 3SAT to Vertex Cover
- Linear blowup reduction from 3SAT to 3COL
- Linear blowup reduction from VC to DOM
- Linear blowup reduction from 3SAT to CLIQ
- Linear blowup reduction from 3SAT to Hamiltonian Cycle.

4 $2^{\Omega(\sqrt{(n)})}$ Lower Bounds from ETH

In order to get a $2^{\Omega(\sqrt{(n)})}$ lower bound for a problem with ETH, we need a reduction from an NP-Complete problem with quadratic blowup.

Some reductions we did in class have quadratic blowup. For example, Planar 3-Coloring required crossover gadgets. The total number of these can in worst case be proportional to n^2. Using results like this, one can derive $2^{\Omega(\sqrt{(n)})}$ bounds on the following problems:

- Planar 3-coloring
- Planar 3-coloring on graphs of degree 4.
- Dominating Set for planar graphs.
- Directed Hamiltonian Cycle for planar graphs.

- Vertex Cover for planar graphs.

Note that although ETH is a hypothesis, we actually really do have an $O(2^n)$ time algorithm for NP-Complete problems. Therefore, we really do have upper bounds for all of the above problems which run in $O(2^{\sqrt{(n)}})$ time. For the details, see the theory of bidimensionality in the papers of Demaine et al. [**?**] [**?**], or the slides of Marx [**?**].

5 Parametrized Complexity

Parametrized problems are problems with a fixed parameter k which is not related to the size of the input n. From ETH, we can get $2^{\Omega(k)n}$ lower bounds.

Theorem 1 *Assuming ETH, Vertex cover, Dominating Set, Clique, and Directed Hamltonian Cycle all require* $2^{\Omega(k)}n^L$ *time to solve.*

Proof. As an example, this proof is for Vertex Cover.

We know that VC requires $2^{\Omega(n)}$ time. If VC_k had an algorithm which ran in $2^{o(k)}n^L$ time, the because $k \leq n$ we would get an $2^{o(n)}n^L$ time algorithm for VC. But this violates the known bound from ETH.

6 $f(k)n^{\Omega(k)}$ Lower Bounds from ETH

Theorem 2 *Let* $f(k)$ *be any function. The* $CLIQ_k$ *and* IS_k *require* $f(k)n^{\Omega(k)}$ *time.*

Proof. By ETH, assume that 3COl requires $2^{\Omega(n)}$ time. The following is a reduction from 3COL to $CLIQ_k$.

- Input a graph $G = (V, E)$. Without loss of generality, we assume that k divides n.
- Divide V into equally sized groups $V_1, ..., V_k$.
- For each i, find all valid 3-colorings of V_i. Create a graph G', with one new vertex for each of these valid 3-colorings. We have $k3^{n/k}$ new vertices.
- For any $i \neq j$, for each pair of compatible colorings between V_i and V_j, add an edge between them

Then G has a 3-coloring if and only if G' has a k-clique. Let k be the largest is can be so that $f(k) \leq n$ and $k^{k/s(k)} \leq n$. Then the algorithm runs in

$$f(k)((k3^{n/k})^{k/s(k)}) \leq nk^{k/s(k)3^{n/s(k)}} \leq n^2 3^{n/s(k(n))} \leq 2^{o}(n)$$

Time.

Definition 3 *Let* A *and* B *be any two* k *parametrized problems. A* k*-linear FPT reduction from A to B is an FPT reduction such that when* (x, k) *is mapped to* (y, k'), $k' = O(k)$.

7 Grid Tiling

Definition 4 (k-Grid Tiling Problem (GRID_k)) *Given a $k \times k$ grid, and $n \in \mathbb{N}$. Each cell $S(i,j)$ in the grid has associated with is a subset of $\{1,...,n\} \times \{1,...,n\}$. Is there a way to pick an ordered pair from each cell so that each adjacent pair of cells horizontally shares their first coordinate, and each adjacent pair of cells vertically shares the second coordinate?*

Theorem 3

- *There is a k-linear FPT reduction from CLIQ_k to GRID_k*
- *GRID_k is W[1]-hard.*
- *For any f, assuming ETH, GRID_k requires $f(k)n^{\Omega(k)}$ time.*

Proof:

- Input a graph and parameter (G,k), where $G=(V,E)$. $V=\{1,...,n\}$. The k for the output GRID problem will be k, and the n will be n. Below, we build the grid.
- For i,j, define $S(i,j)$ as:
  - $S(i,i)=\{(a,a) : 1 \le a \le n\}$
  - for $i<j$, $S(i,j)=\{(a,b) : \{a,b\} \in E\}$

o If G has a k-clique, $\{v_1,...,v_k\}$, then there is a solution to the GRID problem:

- For each i, pick (v_i,v_i) from $S(i,i)$
- For each $i<j$, pick (v_i,v_j) out of $S(i,j)$ and $S(j,i)$.

Definition 5 (List Coloring Problem (LC)) *Given a graph $G=(V,E)$, and for each $v \in V$, a subset L_v of colors $\{1,...,n\}$. Is there a coloring of G where each vertex v has a color in L_v? When this problem is restricted to planar graphs, it is called $\mathsf{PL}-\mathsf{LC}_k$.*

Theorem 4

- *There is a k-lienar FPT reduction from GRID_k to $\mathsf{PL}-\mathsf{LC}_k$*
- *$\mathsf{PL}-\mathsf{LC}_k$ is W[1]-hard*
- *$\mathsf{PL}-\mathsf{LC}_k$ rerquires $f(k)n^{\Omega(k)}$ time*

Proof:

- *Input a GRID problem, which consists of k,j and a $k \times k$ grid of cells called $S(i,j)$ which each have their set of ordered pairs.*
- *For each $a \neq a', b, b' \in \{1,...,n\}$, create a vertex v with $L_v=\{(a,b),(a',b')\}$. Call the set of these vertices X. Note that the size of X is n choose 2 times n^2.*

- *For each* $i \leq j$*, make a vertex* $v_{i,j}$ *with* $L_{v(i,j)} = S(i,j)$.
- *Horizontal edges: for each* $i \leq k-1$*,* $1, \leq j \leq k$*, make a copy of* X*. Put an edge between* $v_{i,j}$ *and each vertex in* X*, and also* $v_{i+1,j}$ *and each vertex in* X*.*
- *Vertical edges: For each* $i \leq k$*, and* $j \leq k$*, make a copy of* X*. Put an edge between* $v_{i,j}$ *and each vertex in* X*, and also* $v_{i+1,j}$ *and each vertex in* X*.*

Definition 6 (k-Grid Tiling LE problem ($GRINDLE_k$)) *Again, we are given a grid with ordered pairs at each cell. Is there a way to pick them so that this time, adjacent cells are increasing in first coordinates on rows, and increasing in second coordinates on columns?*

Theorem 5
- *There is a* k*-linear FPT reduction from* $GRID_k$ *to* $GRINDLE_k$*.*
- $GRINDLE_k$ *is W[1] hard*
- *If we assume ETH, then* $GRINDLE_k$ *requires* $f(k)n^{\Omega(k)}$ *time.*

Definition 7 (Scattered Set Problem (SCAT)) *Given a graph* G *and numbers* k, d*, are there* k *vertices all pairwise distances* $\geq d$*?*

Theorem 6
- *There is a k-linear FPT reduction from* $GRINDLE_k$ *to* SCAT
- *SCAT is W[1] hard*
- *If we assume ETH, the SCAT requires* $f(k)n^{\Omega(k)}$ *time*

Definition 8 (Unit Disk Graph Problem) *Given* P *points in the plane, can you select* k *of the points to center unit disks on without any of the disks intersecting?*

8 Extra Related Problems

- Braverman, Kun Ko, and Weinstein showed that approximating the Nash equilibrium of a game in $n^{O(\log n)}$ time breaks the ETH [**?**]
- Cygan, Fomin, Golovnev, Kulikov, Mihajlin, Pachocki, and Socala showed assuming ETH some lower boudns for some graph problems:
- Deciding if there is a homomorphism between two graphs can't be done in $|V(H)^{O(|V(G)|)}$ time
- There is no $|V(H)^{O(|V(G)|)}$ algorithm for deciding if one graph is a subgraph of another.
- Kowalik, Pilipczuk, Socala, and Wrochna found some lower bounds for graph coloring problems assuming ETH:

- an $(a : b)$ coloring of a graph is a coloring where you assign b colors to each vertex out of a total a colors, so that adjacent verticers have disjoint sets of colors.
- Kowalik et. al. showed that assuming ETH, for any computable f, $(a : b)$ coloring doesn't have an algorithm in $O(f(b)c2^{(\log b)cn})$

References

[1] Braverman, M. et al. "Approximating the best Nash Equilibrium in no(log n)-time breaks the Exponential Time Hypothesis." Electron. Colloquium Comput. Complex. (2014).

[2] Cygan, M., Fomin, F. V., Golovnev, A., Kulikov, A. S., Mihajlin, I., Pachocki, J., & Socała, A. (2017). Tight Lower Bounds on Graph Embedding Problems. Journal of the ACM, 64(3), 1–22. https://doi.org/10.1145/3051094

[3] Bonamy, M., Kowalik, lUkasz, Pilipczuk, M., Socala, A., & Wrochna, M. (2019). Tight Lower Bounds for the Complexity of Multicoloring. ACM Transactions on Computation Theory, 11(3), 1–19. https://doi.org/10.1145/3313906

[4] Erik Demaine, William Gasarch, Mohammad Hajiaghayi *Fun with Hardness: Algorithmmic Lower Bounds*. Not yet Published.

[5] Kazuhisa Makino, Suguru Tamaki, and Masaki Yamamoto. Derandomizing the HSSW algorithm for 3-sat.Algorithmica, 67(2):112–124, 2013.https://doi.org/10.1007/s00453-012-9741-4.

[6] Timon Hertli. 3-sat faster and simpler - Unique-SAT bounds for PPSZhold in general.SIAM Journal on Computing, 43(2):718–729, 2014.https://arxiv.org/abs/1103.2165.

[7] Evgeny Dantsin, Andreas Goerdt, Edward A. Hirsch, Ravi Kannan,Jon M. Kleinberg, Christos H. Papadimitriou, Prabhakar Raghavan, andUwe Sch oning. A deterministic $(2 - 2k + 1)n$ algorithm forksat based onlocal search.Theoretical Computer Science, 289(1):69–83, 2002.https://doi.org/10.1016/S0304-3975(01)00174-8.

[8] Ramamohan Paturi, Pavel Pudl ak, and Francis Zane. Satisfiability cod-ing lemma.Chicago Journal of Theoretical Computer Science, 1999,1999.http://cjtcs.cs.uchicago.edu/articles/1999/11/contents.html.

[9] Uwe Schoning and Jacob Toran.The satisfiability problem. Lehaman'sMedia, 2013.

[10] Russell Impagliazzo and Ramamohan Paturi. On the complexity ofk-SAT.Journal of Computer and System Science, 62(2):367–375, 2001.https://doi.org/10.1006/jcss.2000.1727.

[11] Russell Impagliazzo, Ramamohan Paturi, and Francis Zane. Which problems have strongly exponential complexity?Journal of Computing andSystem Science, 63(4):512–530, 2001.https://cseweb.ucsd.edu/ russell/ipz.pdf.

[12] Erik D. Demaine, Mohammad Taghi Hajiaghayi, and Dimitrios M. Thilikos. Bidimensional theory of bounded-genus graphs.SiAM Journal ofDiscrete Mathematics, 18(3):501–511, 2004.http://www-math.mit.edu/ hajiagha/handle.pdf.

[13] Erik D. Demaine, Fedor V. Fomin, Mohammad Taghi Hajiaghayi, andDimitrios M. Thilikos.Subexponential parameterized algorithms onbounded-genus graphs andH-minor-free graphs.Journal of the Association of Computing Machinery JACM, 52(6):866–893, 2005.http://www-math.mit.edu/ hajiagha/hminorfreeJ15.pdf.

[14] Daniel Marx. The square root phenomenon in planar graphs (slides),2013.http://www.cs.bme.hu/ dmarx/papers/marx-faw-2013-planar.pdf.

[15] Liming Cai and David W. Juedes. On the existence of subexponentialparameterized algorithms.Journal of Computer and System Sciences,67(4):789–807, 2003.https://core.ac.uk/download/pdf/81180403.pdf

[16] Jianer Chen, Iyad A. Kanj, and Ge Xia. Improved upper bounds forvertex cover.Theoretical Computer Science, 411(40-42):3736–3756, 2010.https://doi.org/10.1016/j.tcs.2010.06.026.

[17] Jochen Alber, Hans L. Bodlaender, Henning Fernau, Ton Kloks, and RolfNiedermeier. Fixed parameter algorithms for DOMINATING SET andrelated problems on planar graphs.Algorithmica, 33(4):461–493, 2002.https://doi.org/10.1007/s00453-001-0116-5.

[18] Erik D. Demaine, Fedor V. Fomin, Mohammad Taghi Hajiaghayi, andDimitrios M. Thilikos.Subexponential parameterized algorithms onbounded-genus graphs andH-minor-free graphs.Journal of the Association of Computing Machinery JACM, 52(6):866–893, 2005.http://www-math.mit.edu/ hajiagha/hminorfreeJ15.pdf.

[19] Marek Cygan, Fedor V. Fomin, Lukasz Kowalik, Daniel Lokshtanov,D aaniel Marx, Marcin Pilipczuk, Michal Pilipczuk, and Saket Saurabh.Parameterized Algorithms. Springer, 2015.https://doi.org/10.1007/978-3-319-21275-3.