1 The Orthogonal Vectors Conjecture

In this chapter we have used the 3SUM conjecture as a hardness assumption to obtain quadratic lower bounds. There is one other candidate for a hardness assumption to obtain quadratic lower bounds:

The Orthogonal Vectors Conjecture

Problem 1 *Orthogonal Vectors (*OV*)*
INSTANCE : n *vectors in* $\{0,1\}^d$ *where* $d = O(\log n)$.
QUESTION : Do two of the vectors have an inner product that is 0 mod 2?

A naive algorithm for OV solves it in time $O(n^2 d)$ by trying all possible pairs. Abboud et al. [2] obtained the following slight improvement.

Theorem 1 *There is a randomized algorithm of* OV *that runs in time* $O(n^{2-\Omega(\frac{1}{\log(\frac{d}{n})})})$.

There are no known algorithms for the problem that run in time $n^{2-\epsilon}$ for some $\epsilon > 0$. This leads to the following conjecture, due to Williams [11]. See also Abboud et al. [3], Backurs et al. [4], and Abboud et al. [1]

Conjecture 1 The Orthogonal Vectors Conjecture (OVC) *For all* $\epsilon > 0$*, there is a* $c \geq 1$ *such that* OV *cannot be solved in time* $n^{2-\epsilon}$ *on instances with* $d = c\log(n)$.

We now have several conjectures with rather concrete bounds in them: ETH, SETH, 3SUM, and now OVC. Clearly SETH $\implies$ ETH. Are any other implications known? Yes. Williams [11] showed the following.

Theorem 2 SETH $\implies$ OVC.

The lack of any subquadratic algorithm for OV, and Theorem 2, are evidence for OVC. In addition, OVC holds in several restricted computational models. Kane & Williams [9] show:

1. OV has branching complexity $\tilde{\Theta}(n \cdot \min(n, 2^d))$ for all sufficiently large n, d. (Recall that $\tilde{\Theta}(f(n))$ means that we ignore log factors.)

2. OV has Boolean formula complexity $\tilde{\Theta}(n \cdot \min(n, 2^d))$ over all complete bases of $O(1)$ fan-in.

3. OV requires $\tilde{\Theta}(n \cdot \min(n, 2^d))$ wires, in formulas comprised of gates computing arbitrary symmetric functions of unbounded fan-in.

1.1 What Does OVC Imply and Vice Versa

Theorem 3 *Assume* OVC. *Then the following problems do not have subquadratic algorithms.*

1. *(Backurs & Indyk [4]) Edit Distance: Given 2 strings x, y how many times do you need to delete or insert of replace a letter from either so that at the end the resulting strings are the same. (There are many variants depending on what operations are allowed.)*

2. *(Bringmann [6]) Frechet Distance: This is a measure of similarity between two curves that takes into account the location and ordering of the points on the curve. The formal definition is rather long so we omit it.*

3. *(Backurs & Indyk [5]) Regular Expression Matching: Given a regular expression p and a string t, does p generate some substring of t.*

4. *(Roditty & V. Williams [10]) Approximating the diameter of a graph: See Definition* **??**.

5. *(Burchin et al. [7]) Curve Simplification: This has to do with finding a polygonal curve that is close to the origina. The formal definition is rather long so we omit it.*

While the above results show that many problems are subquadratic assuming OV is subquadratic, this does not necessarily imply that they are *equivalent* to OV. Hence Chen & Williams [8] study equivalences between OV and different problems. They showed the following.

Theorem 4 *Each of the following problems is subquadratic-equivalent to* OV*.*

1. *Min-IP: Given n blue vectors in $\{0, 1\}^d$, and n red vectors in $\{0, 1\}^d$, find the red-blue pair of vectors with minimum inner product.*

2. *Max-IP: Given n blue vectors in $\{0, 1\}^d$, and n red vectors in $\{0, 1\}^d$, find the red-blue pair of vectors with maximum inner product.*

3. *Equals-IP: Given* n *blue vectors in* $\{0,1\}^d$*, and* n *red vectors in* $\{0,1\}^d$*, and an integer* k*, find a red-blue pair of vectors with inner product* k*, or report that none exists.*

4. *Red-Blue-Closest Pair: Let* $p \in [1,2]$ *and* $d = n^{o(1)}$*. Approximating the* ℓ_p*-closest red-blue pair among* n *red points and* n *blue points in* $\mathbb{R}^d$*.*

References

[1] A. Abboud, A. Backurs, and V. V. Williams. Tight hardness results for LCS and other sequence similarity measures. In V. Guruswami, editor, *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17-20 October, 2015*, pages 59–78. IEEE Computer Society, 2015.
`https://doi.org/10.1109/FOCS.2015.14`.

[2] A. Abboud, R. R. Williams, and H. Yu. More applications of the polynomial method to algorithm design. In P. Indyk, editor, *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015, San Diego, CA, USA, January 4-6, 2015*, pages 218–230. SIAM, 2015.
`https://doi.org/10.1137/1.9781611973730.17`.

[3] A. Abboud, V. V. Williams, and O. Weimann. Consequences of faster alignment of sequences. In J. Esparza, P. Fraigniaud, T. Husfeldt, and E. Koutsoupias, editors, *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I*, volume 8572 of *Lecture Notes in Computer Science*, pages 39–51. Springer, 2014.

[4] A. Backurs and P. Indyk. Edit distance cannot be computed in strongly subquadratic time (unless SETH is false). In R. A. Servedio and R. Rubinfeld, editors, *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 51–58. ACM, 2015.
`https://doi.org/10.1145/2746539.2746612`.

[5] A. Backurs and P. Indyk. Which regular expression patterns are hard to match? In I. Dinur, editor, *IEEE 57th Annual Symposium on Foun-*

dations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA, pages 457–466. IEEE Computer Society, 2016.
https://doi.org/10.1109/FOCS.2016.56.

[6] K. Bringmann. Why walking the dog takes time: Frechet distance has no strongly subquadratic algorithms unless SETH fails. In *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, pages 661–670. IEEE Computer Society, 2014. https://doi.org/10.1109/FOCS.2014.76.

[7] K. Buchin, M. Buchin, M. Konzack, W. Mulzer, and A. Schulz. Fine-grained analysis of problems on curves. In A. Blum, editor, *32nd European workshop on Computational Geometry (EuroCG)*, 2016.
https://page.mi.fu-berlin.de/mulzer/pubs/kfrechetEWCG.pdf.

[8] L. Chen and R. Williams. An equivalence class for orthogonal vectors. In T. M. Chan, editor, *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2019, San Diego, California, USA, January 6-9, 2019*, pages 21–40. SIAM, 2019.
https://doi.org/10.1137/1.9781611975482.2.

[9] D. M. Kane and R. R. Williams. The orthogonal vectors conjecture for branching programs and formulas. In A. Blum, editor, *10th Innovations in Theoretical Computer Science Conference, ITCS 2019, January 10-12, 2019, San Diego, California, USA*, volume 124 of *LIPIcs*, pages 48:1–48:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.
https://doi.org/10.4230/LIPIcs.ITCS.2019.48.

[10] L. Roditty and V. V. Williams. Fast approximation algorithms for the diameter and radius of sparse graphs. In D. Boneh, T. Roughgarden, and J. Feigenbaum, editors, *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 515–524. ACM, 2013.
https://doi.org/10.1145/2488608.2488673.

[11] R. Williams. A new algorithm for optimal 2-constraint satisfaction and its implications. *Theor. Comput. Sci.*, 348(2-3):357–365, 2005.
https://doi.org/10.1016/j.tcs.2005.09.023.