1 Extra Related Problems

Cygan et al. [7] showed that, assuming ETH, the following hold:

1. Deciding if there is a homomorphism between two graphs G, H can't be done in $|V(H)^{O(|V(G)|)}$ time
2. There is no $|V(H)^{O(|V(G)|)}$ algorithm for deciding if H is a subgraph G.

We will now look at a graph coloring problem.

Def 1.1 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. One may also say informally that G is $\frac{a}{b}$-colorable. This number is called the *Fractional Chromatic Number*.

The study of fractional chromatic number was motivated as follows.

- Appel et. al [2, 3] showed that every planar graph is 4-colorable. Their proof made extensive use of a computer program to check a massive amount of cases. Robertson et al. [9] had a simpler proof, though it still needed a computer program. In short, the proof is not *human readable*.
- By contrast, the proof that every planar graph is 5-colorable is easy to follow and is clearly human-readable.
- Fractional chromatic number was defined with the goal of finding human-readable proofs that every planar graph is c-colorable for some values of $c < 5$. Cranston & Rabern [6] showed that every planar graph is 4.5-colorable. It is open to lower that.

Bonamy et al. [5] showed the following. Assume ETH. Fix $a, b \in \mathsf{N}$ such that $b \le a$. The problem we are considering is, given a graph G, is it $(a : b)$-colorable. Assume ETH. Then for any computable function f, the problem does not have an $O(f(b)2^{o(\log b)n})$ algorithm.

2 Some Consequences of SETH

1. The Orthogonal Vectors Problem (OVP) is the following: given two sets $A, B \subseteq \{0,1\}^d$ of equal size n, does there exist $\vec{a} \in A, \vec{b} \in B$

with $\vec{a} \cdot \vec{b} \equiv 0 \pmod 2$? It is easy to see that OVP can be solved in $O(n^2 d)$ time. The ORTHOGONAL VECTORS HYPOTHESIS (OVH) is that, for all $\epsilon > 0$, there is no $O(n^{2-\epsilon}$ algorithm for OVP. Williams [10] showed that SETH implies OVH.

2. A lattice $\mathcal{L}$ in R^n is a discrete subgroup of R^n. The CLOSEST VECTOR PROBLEM (CVP) is: given a *lattice* L (specified through a basis) together with a target vector $\vec{v} \in \mathsf{R}^n$, output the $\vec{u} \in L$ that is closest to $\vec{v}$. What do we mean by closest? Let $1 \le p \le \infty$. Then the *p-norm* of a vector $(x_1, \ldots, x_n)$ is

   - $(|x_1|^p + \cdots + |x_n|^p)^{1/p}$ if $p \neq \infty$.
   - $\max_{1 \le i \le n} |x_i|$ if $p = \infty$.

   The common case is $p = 2$ which is the standard Euclidian distance. To indicate that the p-norm is being used, the notation CVP_p is the convention. Aggarwal et al. [1] showed the following: Assuming SETH, for all $\epsilon > 0$, for all $p \notin 2\mathsf{Z}$, there is no $2^{(1-\epsilon)n}$ algorithm for CVP_p. It is unfortunate that they do not have the result for $p = 2$ which is the case of most interest. They comment that the gadgets they use do not exist for even values of p.

3. The SHORTEST VECTOR PROBLEM (SVP) is the following: given a lattice $\mathcal{L}$, output a vector $\vec{v} \in \mathcal{L}$ of minimal norm. Aggarwal et al. [1] showed the following: Assuming SETH, for all $\epsilon > 0$, for all $p \notin 2\mathsf{Z}$, there is no $2^{(1-\epsilon)n}$ algorithm for SVP_p. It is unfortunate that they do not have the result for $p = 2$ which is the case of most interest. This result was obtained by a reduction from CVP_p. The hardness of SVP problem is the basis for most lattice-based crypto systems.

4. Huck Bennet et al. [4] have a survey of open problems on the complexity of lattice problems. We mention one. Show that, assuming SETH, there is no $O(2^{0.99n})$ time algorithm for SVP.

5. Based on their names, one would think that SETH $\Rightarrow$ ETH. While this is true, it is not obvious. The interested reader should see the paper by Impagliazzo et al. [8]. Does ETH $\Rightarrow$ SETH? This is open.

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). In D. Marx, editor, *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms, SODA 2021, Virtual Conference, January 10 - 13, 2021*, pages 1816–1835. SIAM, 2021. `https://doi.org/10.1137/1.9781611976465.109`.

[2] K. Appel and W. Haken. Every planar map is four colorable I: Discharging. *Illinois Journal of Mathematics*, 21:429–490, 1977. `https://projecteuclid.org/euclid.ijm/1256049011`.

[3] K. Appel, W. Haken, and J. Koch. Every planar map is four colorable II: Reducibility. *Illinois Journal of Mathematics*, 21:491–567, 1977. `https://projecteuclid.org/euclid.ijm/1256049012`.

[4] H. Bennett, S. Golovnev, and N. Stephens-Davidowitz. Fine-grained hardness of lattice problems: Open questions, 2020. This is on the Simons Institute Website.

[5] M. Bonamy, L. Kowalik, M. Pilipczuk, A. Socala, and M. Wrochna. Tight lower bounds for the complexity of multicoloring. *ACM Trans. Comput. Theory*, 11(3):13:1–13:19, 2019. `https://doi.org/10.1145/3313906`.

[6] D. Cranston and L. Rabern. Planar graphs are 9/2-colorable and have independence ratio at least 1/3, 2014. paper: `http://arxiv.org/abs/1410.7233`, talk: `http://www.people.vcu.edu/~dcranston/slides/planar-fractional-SFU.pdf`.

[7] M. Cygan, F. V. Fomin, A. Golovnev, A. S. Kulikov, I. Mihajlin, J. Pachocki, and A. Socala. Tight lower bounds on graph embedding problems. *J. ACM*, 64(3):18:1–18:22, 2017. `https://doi.org/10.1145/3051094`.

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

[9] N. Robertson, D. Sanders, P. Seymour, and R. Thomas. The four color theorem. *Journal of Combinatorial Theory (Series B)*, 70:2–44, 1997.

[10] 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`.