1 The Cylinder Conjecture

Suppose we wanted to find a counterexample to the Berman-Hartmanis Isomorphism Conjecture [BH77]. Consider the following family of languages.

$$A_f = \{f(x) : x \in \mathbf{SAT}\}$$

If f is polynomial-time computable, injective and length non-decreasing then A_f is NP-complete. For the rest of this section we will limit ourselves to f that have these properties.

The idea is to find an f *complicated enough* so that A_f is not isomorphic to **SAT**. Deborah Joseph and Paul Young [JY85] first considered this approach in their study of k-creative sets.

In 1995 Stuart Kurtz, Steve Mahaney and Jim Royer [KMR95] define the notion of a scrambling function, a function f such that the range of f does not contain a non-empty paddable language, i.e, where there is a polynomial-time computable and invertible injective function g such that for all strings y, x is in L if and only if $f(x, y)$ is in L. They show

1. For any scrambling function f, A_f is not isomorphic to **SAT**.
2. Relative to a random oracle, scrambling functions exist.

As an immediate corollary, the Berman-Hartmanis conjecture fails relative to a random oracle.

Based on this work, the Berman-Hartmanis conjecture was generally considered likely false as scrambling or other similar functions seemed reasonably likely to exist in the unrelativized world. Or so we thought until 2009 when Manindra Agrawal and Osamu Watanabe [AW09] showed that for the known one-way function candidates f, A_f is isomorphic to **SAT**, at least non-uniformly.

Intuitively, Agrawal and Watanabe show that if f has an easy cylinder than A_f is isomorphic to **SAT**. A cylinder is a way to embed Σ^* into an invertible range of f, informally two easy to compute functions e and g such that for all x, $g(f(e(x))) = x$. The formal definition they need is a bit more technical [AW09, Definition 3]. Agrawal and Watanabe made the following conjecture:

Conjecture (Cylinder Conjecture) If f is easy to compute then f has a non-uniform easy cylinder.

Shortly after Agrawal and Watanabe made their conjecture, Oded Goldreich published [Gol11] a potential counterexample one-way function based on expander graphs. Goldreich's function composes a function with itself several times depending on the input length. Agrawal and Watanabe counter that if one iterates a function with an easy cylinder in this manner, the iterated function should also have an easy cylinder, though they can't prove this point.

The cylinder conjecture remains open and is likely the key to whether the isomorphism conjecture is true in the unrelativized world. While it can't be settled with a relativizing proof, more evidence of the conjecture holding such as a proof that Goldreich's function has an easy cylinder, or a more convincing counterexample would help us better conjecture whether the isomoprhism conjecture may be true.

References

[AW09] Manindra Agrawal and Osamu Watanabe. One-way functions and the berman-hartmanis conjecture. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*, pages 194–202. IEEE Computer Society, 2009.
`https://doi.org/10.1109/CCC.2009.17`.

[BH77] Leonard Berman and Juris Hartmanis. On isomorphism and density of NP and other complete sets. *SIAM Journal on Computing*, 6:305–322, 1977.

[Gol11] Oded Goldreich. A candidate counterexample to the easy cylinders conjecture. In Oded Goldreich, editor, *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation - In Collaboration with Lidor Avigad, Mihir Bellare, Zvika Brakerski, Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin, Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan, Salil Vadhan, Avi Wigderson, David Zuckerman*, volume 6650 of *Lecture Notes in Computer Science*, pages 136–140. Springer, 2011.
`https://doi.org/10.1007/978-3-642-22670-0\_16`.

[JY85] Deborah Joseph and Paul Young. Some remarks on witness functions for nonpolynomial and noncomplete sets in NP. *Theor. Comput. Sci.*, 39:225–237, 1985. https://doi.org/10.1016/0304-3975(85)90140-9.

[KMR95] Stuart A. Kurtz, Stephen R. Mahaney, and James S. Royer. The isomorphism conjecture fails relative to a random oracle. *J. ACM*, 42(2):401–420, 1995. https://doi.org/10.1145/201019.201030.