On the Power of 1-way Functions (Abstract)

Stuart A. Kurtz*
University of Chicago

Stephen R. Mahaney
A. T. & T. Bell Laboratories

James S. Royer†
University of Chicago

The earliest definition of *1-way function* is due to Berman [Ber77], who considered polynomial-time computable, length-increasing, 1-1 functions that do not have a polynomial-time computable inverses. Recently, more powerful notions are considered, e.g., polynomial-time computable, length-increasing, 1-1 functions f such that the probability that a BPP algorithm can compute x from $f(x)$ for a randomly selected x is superpolynomially small [CYa82]. Whatever definition is used, these functions are necessarily easy invert on *some* inputs:

Proposition 1 *If f is a polynomial-time computable, length-increasing, 1-1 function, and if p is a polynomial, then there is a polynomial time algorithm that for sufficiently large n inverts f on at least $p(n)$ strings of length less than n. Therefore, the range of every such function must contain a polynomial-time computable subset of arbitrarily large polynomial census.*

We ask whether or not Proposition 1 is optimal.

Definition 2 *A polynomial-time computable, length-increasing 1-1 function f is an* annihilating function *if every polynomial time decidable subset of the range of f is sparse.*

Polynomial-time computations can do little to invert an annihilating function. The definition, although originally intended as a tool to overthrow the Berman-Hartmanis isomorphism conjecture [BH77, KMR89], can be motivated on a purely cryptographic basis: To defeat a traffic analysis, two sites will send invalid messages to maintain a constant level of virtual traffic, irrespective of the actual traffic. If an eavesdropper could distinguish valid from invalid messages, this strategm would fail. The point behind the definition of an annihilating function is that a polynomial-time algorithm will not permit an eavesdropper to pick out enough valid messages upon which to base a traffic analysis.

We would like to know whether or not annihilating functions exist. It probably doesn't make sense to attack this question directly, as annihilating functions are 1-way functions in at least the Grollman-Selman sense, and so their existence would entail $P \neq UP$ and therefore $P \neq NP$. As a surrogate, we obtain:

*The first author was supported in part by NSF Grant DCR-8602562
†The third author was supported in part by NSF Grant DCR-8602991

S. Goldwasser (Ed.): Advances in Cryptology - CRYPTO '88, LNCS 403, pp. 578-579, 1990.
© Springer-Verlag Berlin Heidelberg 1990

Theorem 3 *With probability 1 relative to a random oracle, annihilating functions exist.*

The instant reaction to Theorem 3 is to ask whether or not it gives us any meaningful insight into the unrelativized case. In general, we do not believe that it is reasonable to base one's intuitions about unrelativized computational world upon relativized worlds. After all, unrestricted relativizations can be used to produce conflicting "worlds."

Random relativizations, on the other hand, cannot conflict with one another. The "measure 1" relativized theory is consistent and well-defined. More importantly, the successful use of pseudo-random number generators in lieu of truly random numbers in probabilistic factoring algorithms makes it seem plausible that computational complexity theory relative to a random oracle is similar to unrelativized computation complexity theory. This intuition was formalized by Bennett and Gill [BG81] as the random oracle hypothesis. Although the formal hypothesis was refuted [Kur83], the informal hypothesis is still compelling, and remains a basis for assigning credibility to random relativizations.

This brings us to a crucial point: do we believe that annihilating functions exist? We are divided ourselves on this question, and await further evidence.

References

[Ber77] L. Berman. *Polynomial Reducibilities and Complete Sets.* PhD thesis, Cornell University, 1977.

[BG81] Charles H. Bennett and John Gill. Relative to a random oracle A, $\mathbf{P}^A \neq \mathbf{NP}^A \neq \mathbf{co\text{-}NP}^A$ with probability 1. *SIAM Journal on Computing*, 10:96–113, February 1981.

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

[CYa82] Andrew C. Yao. Theory and application of trapdoor functions. In *23rd Annual IEEE Symposium on the Foundations of Computer Science*, pages 80–91, 1982.

[KMR89] Stuart A. Kurtz, Stephen R. Mahaney, and James S. Royer. The isomorphism conjecture fails relative to a random oracle. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, pages 157–166, 1989.

[Kur83] Stuart A. Kurtz. On the random oracle hypothesis. *Information and Control*, 57:40–47, 1983.