Electronic Colloquium on Computational Complexity, Comment 1 on Report No. 055 (1998)

Relativizable Pseudorandom Generators and Extractors (Comment to ECCC TR98-055)

Peter Bro Miltersen

September 8, 1998

This comment relates to Trevisan: *Near-Optimal Extractors Using Pseudo-Random Generators*, ECCC TR98-055, in particular to the material in Section 3, page 5, where it is pointed out that the well known Impagliazzo-Wigderson generator, rather surprisingly(!), yields an extractor with better parameters than what was previously known for any explicit construction! Thus, the well known construction actually solves a well known open problem! However, quoting Luca: *"the previously stated property of the Impagliazzo-Wigderson generator was never observed, let alone proved, before, and even though such a property is "implicitly proved" in [IW97], an explicit proof (whether done by this author, or left to the reader) would be long and complicated"*.

The purpose of this comment is to point out that while Luca's remark remains true, the transformation of the proof in [IW97] we need is, in fact, a very well known transformation of proofs in complexity theory, very often left to the reader: One merely has to check that their proof *relativizes*. As is well known, in complexity theory, it is much more noteworthy when a proof does not relativize than when it does, and indeed, by inspection, we see that their proof *does* relativize. In fact, this was explicitly noted in recent work by Dieter van Melkebeek [1].

We now, informally, sketch why the fact that the IW construction relativizes implies that it yields an extractor (we leave to the reader to plug in the appropriate interpretations of "big" and "small").

What Impagliazzo and Wigderson show is the following: There is an efficient hardness-to-randomness generator, i.e. an efficient deterministic algorithm that takes as input (1) the truth-table of a Boolean function with big circuit size and (2) a short random seed, and outputs a longer string which looks random to any small circuit.

Given an oracle A, we replace "big circuit size" with "big A-circuit size" and "any small circuit" with "any small A-circuit". That the IW proof relativizes means that the statement holds, no matter which oracle A is plugged in.

Now suppose that the IW generator is not an extractor. Then, for some source of high min-entropy, the output is not statistically close to uniform. Now fix an oracle A so that it is encoded directly into A which outputs occur with more than their fair share of probability. Now a trivial A-circuit breaks the alleged pseudorandomness, when a random sample of the weak random source is given as input: The circuit just asks A if its input is a high probability string. But, by a counting argument, the random sample corresponds with high probability to a function with big A-circuit complexity, so I shouldn't be able to break it, a contradiction.

References

[1] D. van Melkebeek. "Derandomizing Arthur-Merlin Games". The University of Chicago, Department of Computer Science, Technical Report TR-98-08, July 1998.

ISSN 1433-8092