Errata for:
On Basing One-Way Functions on NP-Hardness

Adi Akavia, Oded Goldreich, Shafi Goldwasser and Dana Moshkovitz

February 8, 2010

This is an errata for our STOC'06 paper, "On Basing One-Way Functions on NP-Hardness" [AGGM06]. We refer to the version dated Feb 28 (2006), which is the basis for our STOC'06 extended abstract.

There is a gap in the proof of our results regarding adaptive reductions, and we currently do not know whether THM 3 (as stated in Sec 2) holds.

The source of trouble is the implicit assumption that the expected size of $T_i^{(k)} = f^{-1}(y_i^{(k)}) \cap h_{k,i,\ell_i^{(k)}}(0^{\ell_i^{(k)}})$ is $2^{\ell_i^{(k)}} \cdot |f^{-1}(y_i^{(k)})|$ (cf., also Eq (2)). This would have been true if $y_i^{(k)}$ is fixed independently of $h_{k,i,\ell_i^{(k)}}$ (or, in other words, if $h_{k,i,\ell_i^{(k)}}$ is uniformly distributed given $y_i^{(k)}$), and $y_i^{(k)}$ is indeed fixed if the prover did not cheat in prior rounds of copy k (i.e., $A_j^{(k)} = T_j^{(k)}$ for every $j < i$). However, if such a cheating occurs wrt copy k, then the cheating prover may set $y_i^{(k)}$ (among a few possibilities) based on the value of all h's including $h_{k,i,\ell_i^{(k)}}$. (Specifically, the prover may choose to cheat in round i' of copy k if this allows it to select an answer that both leads the reduction to a wrong answer and allows $T_j^{(k)}$ to be larger than expected.) Consequently, for such k's $T_i^{(k)}$ may be larger than we expect, and this excess may be used to claim smaller sizes for additional k' (i.e., have $A_j^{(k')} \subset T_j^{(k')}$).

We note that the "warm-up" case discussed in the beginning of Sec 2.1 (i.e., f having polynomially bounded preimage size) remains intact, and so all assertions made wrt adaptive reductions are valid when applied to this special case. We also note that the said gap does not effect our analysis of non-adaptove reductions (in Sec 2.2 culminating in Thm 5).

References

[AGGM06] A. Akavia, S. Goldwasser, O. Goldreich, and D. Moshkovitz. On Basing One-Way Functions on NP-Hardness. In *proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC '06)*, pages 701–710, 2006.