Electronic Colloquium on Computational Complexity - Reports Series 1995 - available via:

Comment 01 on ECCC TR95-050

FTP: ftp.eccc.uni-trier.de:/pub/eccc/

WWW: http://www.eccc.uni-trier.de/eccc/

Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

Errata to ECCC Report 95-050 "On Yao's XOR-Lemma"

Oded Goldreich* Noam Nisan† Avi Wigderson‡

December 8, 1995

The purpose of this errata is to correct some typos in the proof of Lemma 12.

- On page 23, the probability bound in Claim 12.3 should be $(1/2)+2\epsilon$ (rather than $(1/2)+(\epsilon/2)$).
- On page 23, second line of the proof, ζ_z should be ζ_x.
- On page 24, the last line in the bound on the expectation (of $\sum_{x\in C}\zeta_x w_x$) should be $\rho(n)\cdot[(1/2)+\epsilon]$ (rather than $\rho(n)\cdot[(1/2)-\epsilon]$).
- On page 24, in the Chernoff bound inequality, the treshold should be $\rho(n)\cdot[(1/2)+(4\epsilon/3)]$ (rather than $\rho(n)\cdot[(1/2)-(3\epsilon/4)]$).
- On page 24, in the one-before-last sentence of the proof of Claim 12.3, the numerator should be bounded by $\rho(n)\cdot[(1/2)+(4\epsilon/3)]$ (rather than by $\rho(n)\cdot[(1/2)-(3\epsilon/4)]$).
- On page 24, in the last inequality, the bound should be $(1/2)+2\epsilon$ (rather than $(1/2)+(\epsilon/2)$).

Below we reproduce the entire corrected text (from Claim 12.3 to the end of the proof of Lemma 12).

claim 12.3: Let C_n be a circuit of size $s'(n)$. Then,

$$\mathrm{Prob}[C_n(X_n)=f(X_n)|X_n\in R_n] < \frac{1}{2}+2\epsilon$$

for all but a $2^{-(s'(n)^2+1)}$ measure of the choices of R_n.

proof: We define the same random variables $\zeta_x=\zeta_x(R_n)$ as in the proof of the previous claim; $\zeta_x(R_n)=1$ if $x\in R_n$ and $\zeta_x(R_n)=0$ otherwise. Also, as before, $w_x \stackrel{\rm def}{=} \mathrm{Prob}[X_n=x]$, for every $x\in\{0,1\}^n$. Let C be the set of inputs on which C_n correctly computes f; namely,

$$C \stackrel{\rm def}{=} \{x : C_n(x)=f(x)\}$$

For every choice of R_n, we are interested in the probability

$$\mathrm{Prob}[X_n\in C|X_n\in R_n] = \frac{\mathrm{Prob}[X_n\in C \wedge X_n\in R_n]}{\mathrm{Prob}[X_n\in R_n]} \tag{12}$$

We first determine the expected value of the numerator of Eq. (12), where the expectation is taken over the possible choices of R_n. We rewrite the numerator as $\sum_{x\in C}\zeta_x(R_n)\cdot w_x$, and bound it as follows

$$\mathrm{E}[\sum_{x\in C}\zeta_x\cdot w_x] \;=\; \sum_{x\in C} p(x)\cdot w_x$$

*Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel.

†Institute for Computer Science, Hebrew University, Jerusalem, Israel.

‡Institute for Computer Science, Hebrew University, Jerusalem, Israel.

$$
\begin{aligned}
&= \sum_{x\in C} \frac{\rho(n)\cdot \mathrm{Prob}[Y_n = x]}{\mathrm{Prob}[X_n = x]} \cdot \mathrm{Prob}[X_n = x] \\
&= \rho(n)\cdot \mathrm{Prob}[Y_n \in C] \\
&\leq \rho(n)\cdot \left(\frac{1}{2}+\epsilon\right)
\end{aligned}
$$

where the last inequality is due to the hypothesis regarding Y_n. Next, we use Chernoff bound and get

$$
\mathrm{Prob}[\sum_{x\in C} w_x\zeta_x > (\frac{1}{2}+\frac{4\epsilon}{3})\cdot\rho(n)] < \exp\left(-\Omega\left(\frac{\epsilon^2\rho(n)}{\max_x\{w_x\}}\right)\right)
$$

Now, using the simplifying assumptions regarding the w_x's and ϵ, the latter expression is bounded by $\exp(-\sqrt{s(n)/\mathrm{poly}(n)})$. Thus, for all but a $\exp(-s'(n)^2+2)$ measure of the R_n's the numerator of Eq. (12) is bounded above by $(\frac{1}{2}+\frac{4\epsilon}{3})\cdot\rho(n)$. Using the previous claim, we conclude that for a similar measure of R_n's the denumerator of Eq. (12) is bounded below by $(1-\frac{\epsilon}{3})\cdot\rho(n)$. The claim follows. □

The lemma now follows by combining the above three claims. Claim 12.1 provides us with a suitable $\mathbf{Y}$ for which we apply the probabilistic construction, whereas Claims 12.2 and 12.3 establish the existence of a set R_n such that both

$$
\mathrm{Prob}[X_n \in R_n] > (1-o(1))\cdot\rho(n)
$$

and

$$
\mathrm{Prob}[C_n(X_n) = f(X_n) | X_n \in R_n] < \frac{1}{2} + 2\epsilon
$$

for all $2^{s'(n)^2}$ possible circuits, C_n, of size $s'(n)$. The lemma follows. ■