Low-error two-source extractors for polynomial min-entropy

Avraham Ben-Aroya* Dean Doron† Amnon Ta-Shma‡

The paper contained an error and was retracted.

The aim of this paper was to present a new two-source extractor for min-entropy n^α for some $\alpha < 1$ having exponentially-small error. Say we are given two independent sources X and Y. The technique was to condense Y using a somewhere-random condenser to a somewhere-random source with t rows, where one of the rows has a high min-entropy rate. Then, in order to break correlations between the rows, we would use an advice correlation breaker (following the work of [2] and also techniques developed in [3], for example). The advice correlation breaker that we constructed may be of independent interest in case the number of rows is small.

Specifically:

Definition. *An $((n,k) \times (\ell, \alpha\ell) \to_\varepsilon m)$ t-NM advice correlation breaker is a function*

$$\mathsf{AdvCB} : \{0,1\}^n \times \{0,1\}^\ell \times \{0,1\}^a \to \{0,1\}^m$$

such that for every random variables $\left\{X^{(j)}\right\}_{0 \le j \le t}$, where $X^{(j)}$ is distributed over $\{0,1\}^n$, and for every random variables $\left\{Y^{(j)}\right\}_{0 \le j \le t}$ that are distributed over $\{0,1\}^\ell$, and for every $t+1$ strings $adv^{(0)}, \ldots, adv^{(t)} \in \{0,1\}^a$, the following holds. Denote $X = X^{(0)}, Y = Y^{(0)}$. If

- $\left\{X^{(j)}\right\}_{0 \le j \le t}$ *are independent of* $\left\{Y^{(j)}\right\}_{0 \le j \le t}$,
- $H_\infty(X) \ge k$,
- $H_\infty(Y) \ge \alpha\ell$, *and,*
- $adv^{(0)} \notin \left\{adv^{(j)}\right\}_{j \in [t]}$,

then

$$\mathsf{AdvCB}\left(X, Y, adv^{(0)}\right) \circ \left\{\mathsf{AdvCB}\left(X^{(j)}, Y^{(j)}, adv^{(j)}\right)\right\}_{j \in [t]} \approx_\varepsilon U_m \times \left\{\mathsf{AdvCB}\left(X^{(j)}, Y^{(j)}, adv^{(j)}\right)\right\}_{j \in [t]}.$$

*The Blavatnik School of Computer Science, Tel-Aviv University, Tel Aviv 69978, Israel. Supported by the Israel science Foundation grant no. 994/14 and by the United States – Israel Binational Science Foundation grant no. 2010120.

†The Blavatnik School of Computer Science, Tel-Aviv University, Tel Aviv 69978, Israel. Email: deandoron@mail.tau.ac.il. Supported by the Israel science Foundation grant no. 994/14 and by the United States – Israel Binational Science Foundation grant no. 2010120.

‡The Blavatnik School of Computer Science, Tel-Aviv University, Tel Aviv 69978, Israel. Email: amnon@tau.ac.il. Supported by the Israel science Foundation grant no. 994/14 and by the United States – Israel Binational Science Foundation grant no. 2010120.

Theorem. *There exist constants* $c_{\mathsf{adv}} > 1$, $c_{\mathsf{gap}} > 0$ *such that for every* $n, t \leq n, \zeta > 0$, $k \geq c_{\mathsf{adv}} t^5 \log \frac{n}{\zeta}$ *and* $\alpha \geq 1 - \frac{c_{\mathsf{gap}}}{t^3}$, *there exists a* $((n,k) \times (\ell, \alpha\ell) \to_\zeta m)$ *t-NM advice correlation breaker*

$$\mathsf{AdvCB} : \{0,1\}^n \times \{0,1\}^\ell \times \{0,1\}^{\log t} \to \{0,1\}^m$$

with seed length $\ell = c_{\mathsf{adv}} t^3 \log \frac{n}{\zeta}$ *and output length* $m \leq \frac{k}{c_{\mathsf{adv}} t^3} - c_{\mathsf{adv}} t \log \frac{n}{\zeta}$.

This theorem is correct. However, we did not apply it in a correct way. In order to apply the above correlation breaker, the condenser must output t rows, one with density at least $1 - \frac{1}{t}$. However, we do not know how to build such a condenser, and [1] showed us it cannot be built in a deterministic way.

References

[1] Eshan Chattopadhyay, Gil Cohen, and Xin Li. Personal communication, July 2016.

[2] Gil Cohen. Making the most of advice: New correlation breakers and their applications. *ECCC*, 2016.

[3] Xin Li. Extractors for a constant number of independent sources with polylogarithmic min-entropy. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 100–109. IEEE, 2013.