Randomness from independent processes

https://arxiv.org/abs/2510.05203

Martin Sandfuchs[1], Carla Ferradini[1], and Renato Renner[1]

[1]Institute for Theoretical Physics, ETH Zurich

Motivation and setup

Question: ~~Does uniform randomness exist?~~
Under what assumptions can we prove that uniform randomness exists?

Recall: Randomness extraction (Tuesday)

Let ρ_{XE} be a cq state. Then, there exists a function $\mathrm{Ext} : \mathcal{X} \times \mathcal{S} \to \mathcal{Z}$, such that

$$\frac{1}{2}\left\|\rho_{\mathrm{Ext}(X,S)SE} - \omega_Z \otimes \rho_{SE}\right\|_1 \leq \frac{1}{2}\sqrt{2^{\log|\mathcal{Z}| - H_{\min}(X|E)_\rho}},$$

where $\omega_Z = \frac{1}{|\mathcal{Z}|}\mathbb{1}_Z$ and S is a uniform and independent random seed.

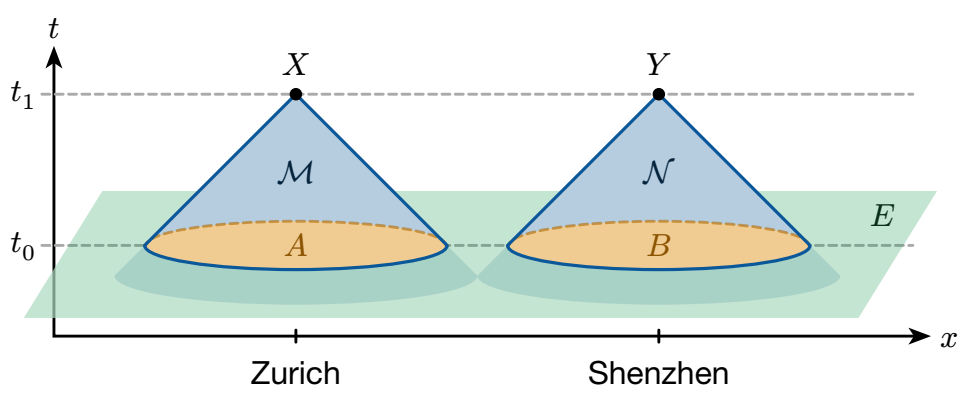
Idea: Use a non-uniform seed.

Definition. Let $\rho_{XYE_1E_2} = \rho_{XE_1} \otimes \rho_{YE_2}$ be classical on X and Y. We call Ext a (k_1, k_2, ε) *two-source extractor* if

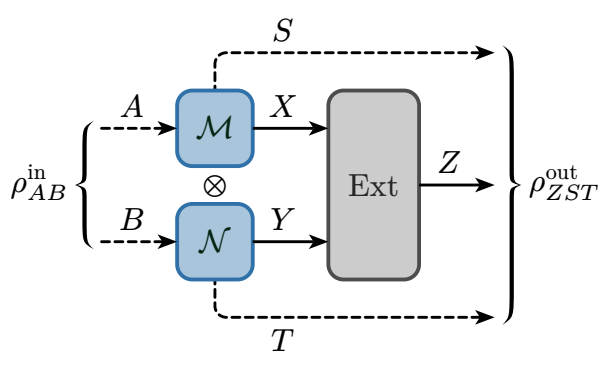
$$\frac{1}{2}\left\|\rho_{\mathrm{Ext}(X,Y)E_1E_2} - \omega_Z \otimes \rho_{E_1E_2}\right\|_1 \leq \varepsilon$$

whenever $H_{\min}(X|E_1) \geq k_1$ and $H_{\min}(Y|E_2) \geq k_2$.

Physical setting



Mathematical description



Independence also holds without space-like separation if the processes happen in isolated laboratories.

Two-process extractors

Definition. Let $\mathcal{M}_{XS|A}$ and $\mathcal{N}_{YT|B}$ be two CPTP maps and let ρ^{in}_{AB} be a pure state. Assume that

$$H_{\min}(X|SB)_{\mathcal{M}[\rho^{\mathrm{in}}]} \geq k_1 \quad \text{and} \quad H_{\min}(Y|TA)_{\mathcal{N}[\rho^{\mathrm{in}}]} \geq k_2.$$

We call $\mathrm{Ext} : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ a (k_1, k_2, ε) *two-process extractor* if

$$\frac{1}{2}\left\|\rho^{\mathrm{out}}_{ZST} - \omega_Z \otimes \rho^{\mathrm{out}}_{ST}\right\|_1 \leq \varepsilon,$$

where $\rho^{\mathrm{out}}_{ZST} = \mathrm{Ext}_{Z|XY} \circ \left(\mathcal{M}_{XS|A} \otimes \mathcal{N}_{YT|B}\right)[\rho^{\mathrm{in}}_{AB}]$.

Since the initial state ρ^{in}_{AB} is pure, we can think of B as a coherent copy of A. Hence, $H_{\min}(X|SB)_{\mathcal{M}[\rho^{\mathrm{in}}]} \geq k_1$ requires that the output of $\mathcal{M}$ is unpredictable, even when the input is known.

Challenge. Due to entanglement in ρ^{in}_{AB}, there can be strong correlations between X and Y.

If $\rho^{\mathrm{in}}_{AB} = \sum_i p_i \rho^i_A \otimes \rho^i_B$ were separable, then

$$\left(\mathcal{M}_{XS|A} \otimes \mathcal{N}_{YT|B}\right)[\rho^{\mathrm{in}}_{AB}] = \sum_i p_i \mathcal{M}_{XS|A}[\rho^i_A] \otimes \mathcal{N}_{YT|B}[\rho^i_B].$$

For separable inputs, our model reduces to the previously studied Markov chains $XS \leftrightarrow I \to YT$ (after a conditioning register I is introduced).

However, Bell's Theorem tells us that entangled states can produce much stronger correlations!

Results

Feasibility of two-process extraction

Definition. Let $\mathcal{K} = \{K_i\}_{i=1}^m$ be a set of $n \times n$ matrices with entries in $\{0,1\}$. Define

$$\mathrm{DEOR}^{\mathcal{K}} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$$
$$(x, y) \mapsto (x^T K_1 y) \cdots (x^T K_m y).$$

Result 1. Let $r \in \mathbb{N}_0$ be such that $\mathrm{rank}(\sum_{i \in I} K_i) \geq n - r$ for all $\emptyset \neq I \subseteq \{1, ..., m\}$. Then, $\mathrm{DEOR}^{\mathcal{K}}$ is a (k_1, k_2, ε) two-process extractor with

$$\varepsilon = \frac{1}{2}\sqrt{2^{2m+n+r-k_1-k_2}}.$$

There are constructions achieving $r = 0$ for any $m \leq n$.

Classical randomness extraction

Surprisingly, two-process extractors also give new insights into purely classical randomness extraction:

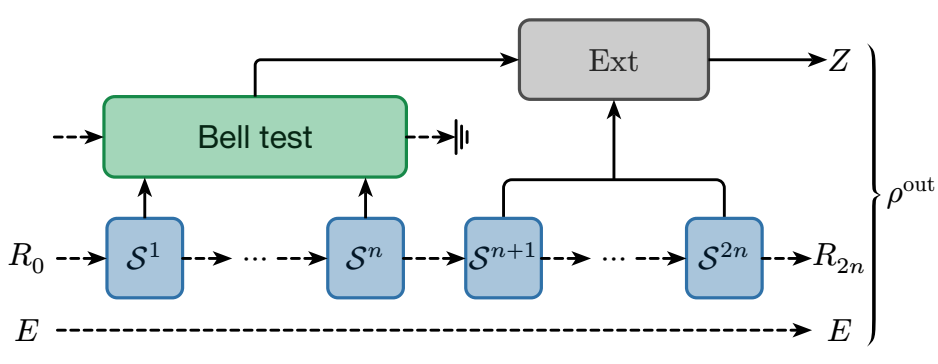
Result 2. Let $p(x, y)$ be a probability distribution and Ext be a (k_1, k_2, ε) two-process extractor. Define

$$\eta_{XB} := \sum_{x,y,y'} p(x)|x\rangle\langle x|_X \otimes |\eta_x\rangle\langle\eta_x|_B \quad \text{with} \quad |\eta_x\rangle_B = \sum_y \sqrt{p(y|x)}|y\rangle_B$$
$$\text{and} \quad \nu_{YA} := \sum_{x,x',y} p(y)|y\rangle\langle y|_Y \otimes |\nu_y\rangle\langle\nu_y|_A \quad \text{with} \quad |\nu_y\rangle_A = \sum_x \sqrt{p(x|y)}|x\rangle_A.$$

If $H_{\min}(X|B)_\eta \geq k_1$ and $H_{\min}(Y|A)_\nu \geq k_2$, then Ext can extract from $p(x, y)$ with error ε.

In Result 2, there is no assumption on the structure of $p(x, y)$. In particular, Result 2 allows for extraction from correlated sources.

Application to randomness amplification

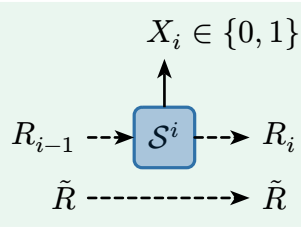


Goal:
$$\frac{1}{2}\left\|\rho^{\mathrm{out}}_{ZR_{2n}E} - \omega_Z \otimes \rho^{\mathrm{out}}_{R_{2n}E}\right\|_1 \leq \varepsilon$$

Previously: Only classical side-information about the source was possible, that is, $R_0 ... R_{2n}$ needed to be classical. We can now lift this restriction.

Definition *(Quantum SV-source)*. We call a sequence of channels $\{\mathcal{S}^i_{X_iR_i|R_{i-1}}\}_i$ a quantum SV-source with bias μ if

$$H_{\min}(X_i|\tilde{R})_{\mathcal{S}^i[\rho]} \geq -\log\left(\frac{1}{2} + \mu\right) \quad \forall i, \rho_{R_{i-1}\tilde{R}}.$$



Result 3 *(Informal)*. Device-independent randomness amplification of a quantum SV-source is possible.

Take-home message

Perfect randomness can be generated under surprisingly weak assumptions!

Outlook

Main limitation: The $\mathrm{DEOR}^{\mathcal{K}}$ extractor requires that $k_1 + k_2 > n$.

In the classical setting, $k_1 = k_2 = O(\log n)$ is enough. That is, there are functions $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ such that for $k = O(\log n)$

$$\max_{p(x),q(y) \leq 2^{-k}} \left|\sum_{x,y} (-1)^{\mathrm{Ext}(x,y)} p(x)q(y)\right| \leq \varepsilon. \tag{1}$$

In our setting, we require

$$\max_{M(x),N(y) \leq 2^{-k}} \left\|\sum_{x,y} (-1)^{\mathrm{Ext}(x,y)} M(x) \otimes N(y)\right\|_\infty \leq \varepsilon. \tag{2}$$

Open problem. Does (1) $\Rightarrow$ (2)?

Questions?