From the compression theorem to the undecidability of approximating the quantum value of a game

Omar Fawzi

ENS DE LYON

GDT Connes-Tsirelson, Lyon, April 16th, 2020

arXiv:2001.04383

Recall the setup

Theorem (Game value at least as hard as halting)

For all Turing machines $\mathcal{M}$, there exists a game $\mathfrak{G}_{\mathcal{M}}$ such that

- *If $\mathcal{M}$ halts on empty tape, then $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = 1$*
- *If $\mathcal{M}$ does not halt on empty tape, then $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) \leq \frac{1}{2}$*

Moreover, a description of the game $\mathfrak{G}_{\mathcal{M}}$ can be computed in polynomial time in the size of the description of $\mathcal{M}$.

$\mathfrak{G}$ is described by:

- A probability measure μ on inputs $\mathcal{X} \times \mathcal{Y}$, $\mu(x, y)$: prob. of choosing questions x, y
- A verification predicate $D : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$: $D(x, y, a, b) = 1$ means win

$$\mathrm{val}^*(\mathfrak{G}) = \sup_{p \in C_{q\otimes}} \sum_{x,y} \mu(x, y) \sum_{a,b} D(x, y, a, b) p_{abxy}$$

Recall the setup

Theorem (Game value at least as hard as halting)

For all Turing machines $\mathcal{M}$, there exists a game $\mathfrak{G}_{\mathcal{M}}$ such that

- *If $\mathcal{M}$ halts on empty tape, then $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = 1$*
- *If $\mathcal{M}$ does not halt on empty tape, then $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) \leq \frac{1}{2}$*

Moreover, a description of the game $\mathfrak{G}_{\mathcal{M}}$ can be computed in polynomial time in the size of the description of $\mathcal{M}$.

$\mathfrak{G}$ is described by:

- A probability measure μ on inputs $\mathcal{X} \times \mathcal{Y}$, $\mu(x, y)$: prob. of choosing questions x, y
- A verification predicate $D : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$: $D(x, y, a, b) = 1$ means win

$$\mathrm{val}^*(\mathfrak{G}) = \sup_{p \in C_{q\otimes}} \sum_{x,y} \mu(x, y) \sum_{a,b} D(x, y, a, b) p_{abxy}$$

Remark:
Let $\mathscr{E}(\mathfrak{G}, p) :=$ min. dimension needed for winning prob $\geq p$ (can be $+\infty$)
Statement of the form $\mathscr{E}(\mathfrak{G}, \mathrm{val}^*(\mathfrak{G}) - \frac{1}{4}) \leq f(\mathfrak{G})$ with f computable contradicts theorem
$\Rightarrow$ Need to show existence of games $\mathfrak{G}$ that need entanglement $\gg$ size of description of $\mathfrak{G}$

A few things about Turing machines

- A k-input Turing machine (TM) $\mathcal{M}$ computes a partial function $f : (\{0,1\}^*)^k \to \{0,1\}^*$, that we also call $\mathcal{M}$. If $\mathcal{M}$ does not halt on $x_1, \ldots, x_k$, we set $\mathcal{M}(x_1, \ldots, x_k) = \perp$
- A TM $\mathcal{M}$ (a tuple with states and transition rules) can be described by a bitstring $\overline{\mathcal{M}} \in \{0,1\}^*$. We use $|\mathcal{M}|$ for the length of the bitstring $\overline{\mathcal{M}}$
- Conversely any $\alpha \in \{0,1\}^*$ can be interpreted as a k-input TM $[\alpha]_k$
- It is possible to simulate TMs from their description

Theorem (Efficient universal Turing machines)

For any k, there exists a 2-input TM $\mathcal{U}_k$ such that for any $\alpha \in \{0,1\}^*, x \in (\{0,1\}^*)^k$, $\mathcal{U}_k(\alpha, k) = [\alpha]_k(x)$. $\mathcal{U}_k(\alpha, x)$ halts within $C_{k,\alpha} T \log T$ steps if $[\alpha]_k(x)$ halts in T steps.

- $\mathrm{TIME}_{\mathcal{M},x}$ denotes the running time of $\mathcal{M}$ on input x (∞ if does not halt)
- In the rest of the talk, we will not always make the distinction between $\mathcal{M}$ and its description $\overline{\mathcal{M}}$

Describing families of games

Will need families of games described by Turing machines

Definition

A *normal form verifier* (NFV) is a pair $\mathcal{V} = (\mathcal{S}, \mathcal{D})$ of Turing machines.

- $\mathcal{S}$ is called a *sampler* (full definition is complicated and not important for today)
  On input starting with $n \in \mathbb{N}$ outputs a description of
  a probability distribution $\mu_{\mathcal{S},n}$ on $\{0,1\}^{\leq \mathrm{RAND}_{\mathcal{S}}(n)} \times \{0,1\}^{\leq \mathrm{RAND}_{\mathcal{S}}(n)}$
- $\mathcal{D}$ is called a *decider* and is a 5-input Turing machine
  Input of the form (n, x, y, a, b) with $n \in \mathbb{N}$ and $x, y, a, b \in \{0,1\}^*$
  $\mathrm{TIME}_{\mathcal{D}}(n)$: max. running time on inputs (n, x, y, a, b)
  $\mathcal{D}$ outputs 0 or 1

A normal form verifier defines a family of nonlocal games for every n

Definition

$\mathcal{V}$ defines the games $\{\mathcal{V}_n\}$ with

- question sets $\mathcal{X} = \mathcal{Y} = \{0,1\}^{\leq \mathrm{RAND}_{\mathcal{S}}(n)}$
- answer sets $\mathcal{A} = \mathcal{B} = \{0,1\}^{\leq \mathrm{TIME}_{\mathcal{D}}(n)}$
- prob distribution on questions $\mu_{\mathcal{S},n}$
- decision predicate is $\mathcal{D}(n, ., ., ., .)$

$\mathrm{RAND}_{\mathcal{S}}(n)$ and $\mathrm{TIME}_{\mathcal{D}}(n)$ will be polynomials in n

The compression theorem: overview

The main theorem of the paper is:

Theorem (Compression theorem)

There exists a polynomial-time Turing machine Compress *that takes as input a NFV* $\mathcal{V} = (\mathcal{S}, \mathcal{D})$ *and outputs another NFV* $\mathcal{V}' = (\mathcal{S}', \mathcal{D}')$ *satisfying for all* $n \in \mathbb{N}$

1. *If* $\mathrm{val}^*(\mathcal{V}_{2^n}) = 1$*, then* $\mathrm{val}^*(\mathcal{V}'_n) = 1$
2. *If* $\mathrm{val}^*(\mathcal{V}_{2^n}) \leq \frac{1}{2}$*, then* $\mathrm{val}^*(\mathcal{V}'_n) \leq \frac{1}{2}$
3. $\mathscr{E}(\mathcal{V}'_n, \frac{1}{2}) \geq \max\{\mathscr{E}(\mathcal{V}_{2^n}, \frac{1}{2}), 2^{2^{\Omega(n)}}\}$

$\mathscr{E}(\mathfrak{G}, \frac{1}{2}) :=$ min. dimension needed to get a winning prob $\geq \frac{1}{2}$
The sampler $\mathcal{S}'$ does not depend on $\mathcal{V}$

Today: Compression theorem $\Longrightarrow$ Game value as hard as halting

The compression theorem: overview

The main theorem of the paper is:

Theorem (Compression theorem)

There exists a polynomial-time Turing machine Compress *that takes as input a NFV* $\mathcal{V} = (\mathcal{S}, \mathcal{D})$ *and outputs another NFV* $\mathcal{V}' = (\mathcal{S}', \mathcal{D}')$ *satisfying for all* $n \in \mathbb{N}$

1. *If* $\mathrm{val}^*(\mathcal{V}_{2^n}) = 1$, *then* $\mathrm{val}^*(\mathcal{V}'_n) = 1$
2. *If* $\mathrm{val}^*(\mathcal{V}_{2^n}) \leq \frac{1}{2}$, *then* $\mathrm{val}^*(\mathcal{V}'_n) \leq \frac{1}{2}$
3. $\mathscr{E}(\mathcal{V}'_n, \frac{1}{2}) \geq \max\{\mathscr{E}(\mathcal{V}_{2^n}, \frac{1}{2}), 2^{2^{\Omega(n)}}\}$

$\mathscr{E}(\mathfrak{G}, \frac{1}{2}) :=$ min. dimension needed to get a winning prob $\geq \frac{1}{2}$
The sampler $\mathcal{S}'$ does not depend on $\mathcal{V}$

Today: Compression theorem $\implies$ Game value as hard as halting

Sketch:

- Given $\mathcal{M}$, construct a NFV $\mathcal{V}^{\mathcal{M}} = (\mathcal{S}^{\mathcal{M}}, \mathcal{D}^{\mathcal{M}})$ with $\mathcal{D}^{\mathcal{M}}$ working as follows:
  On input (n, x, y, a, b), execute $\mathcal{M}$ for n steps, if halts $\Rightarrow$ output 1
  Else compute a description of $\mathcal{V}' = (\mathcal{S}', \mathcal{D}') :=$ Compress$(\mathcal{V}^{\mathcal{M}})$ and output $\mathcal{D}'(n, x, y, a, b)$
- If $\mathcal{M}$ halts in T steps, then $n \geq T$, $\mathrm{val}^*(\mathcal{V}^{\mathcal{M}}_n) = 1$
  For $n < T$, $\mathrm{val}^*(\mathcal{V}^{\mathcal{M}}_n) = \mathrm{val}^*(\mathcal{V}^{\mathcal{M}}_{2^n}) = \mathrm{val}^*(\mathcal{V}^{\mathcal{M}}_{2^{2^n}}) = \cdots = 1$
- If $\mathcal{M}$ does not halt, then for any n
  $\mathscr{E}(\mathcal{V}'_n, \frac{1}{2}) \geq \mathscr{E}(\mathcal{V}^{\mathcal{M}}_{2^n}, \frac{1}{2}) \geq \cdots \geq 2^{2^{\cdots 2^n}}$
  $\mathscr{E}(\mathcal{V}'_n, \frac{1}{2}) = +\infty \quad \implies \quad \mathrm{val}^*(\mathcal{V}^{\mathcal{M}}_n) \leq \frac{1}{2}$

The compression theorem in more detail

Definition

$\mathcal{V} = (\mathcal{S}, \mathcal{D})$ is λ bounded if

1. $|\mathcal{V}| \leq \lambda$
2. For all n, $\mathsf{TIME}_{\mathcal{D}}(n), \mathsf{RAND}_{\mathcal{S}}(n) \leq (\lambda n)^{\lambda}$
   i.e., the game $\mathcal{V}_n$ has questions and answers bitstrings of length $\leq (\lambda n)^{\lambda}$

Theorem (Compression theorem)

For every $\lambda \in \mathbb{N}_+$ (parameter that will govern the game families for which compression works) there exists a TM $\mathsf{Compress}_{\lambda}$

$$\mathcal{V} = (\mathcal{S}, \mathcal{D}) \quad \to \quad \mathsf{Compress}_{\lambda} \quad \to \quad \mathcal{V}^{\mathrm{COMPR}} = (\mathcal{S}^{\mathrm{COMPR}}, \mathcal{D}^{\mathrm{COMPR}})$$

- *Description of* $\mathsf{Compress}_{\lambda}$ *can be computed in time* $\mathrm{poly}(\log \lambda)$
- $\mathsf{Compress}_{\lambda}$ *runs in time polynomial in* $|\mathcal{V}|$ *and* $\log \lambda$
- $|\mathcal{D}^{\mathrm{COMPR}}| = \mathrm{poly}(|\mathcal{V}|, \log \lambda)$ *and* $|\mathcal{S}^{\mathrm{COMPR}}| = \mathrm{poly}(\log \lambda)$
- $\mathsf{TIME}_{\mathcal{D}^{\mathrm{COMPR}}}(n) = \mathrm{poly}(n, |\mathcal{V}|, \lambda)$ *and* $\mathsf{RAND}_{\mathcal{S}^{\mathrm{COMPR}}}(n) = \mathrm{poly}(n, \lambda)$

and if $\mathcal{V}$ is λ-bounded then for all $n \geq n_0$ (universal constant)

- *If* $\mathrm{val}^*(\mathcal{V}_{2^n}) = 1$, *then* $\mathrm{val}^*(\mathcal{V}_n^{\mathrm{COMPR}}) = 1$
- *If* $\mathrm{val}^*(\mathcal{V}_{2^n}) \leq \frac{1}{2}$, *then* $\mathrm{val}^*(\mathcal{V}_n^{\mathrm{COMPR}}) \leq \frac{1}{2}$
- $\mathscr{E}(\mathcal{V}'_n, \frac{1}{2}) \geq \max\{\mathscr{E}(\mathcal{V}_{2^n}, \frac{1}{2}), \frac{1}{2} 2^{\lambda 2^{\lambda n}}\}$

Using the compression theorem

For every TM $\mathcal{M}$ and parameters λ, Δ, we construct a **TM $\mathcal{F}$**:

- **Input:** description of $\mathcal{D}$ of 5-input TM
- **Output:** description of $\mathcal{D}'$ of a 5-input TM that works as follows
  On input (n, x, y, a, b)
  1. Run $\mathcal{M}$ on empty tape for n steps. If $\mathcal{M}$ halts, accept
  2. Else $\mathcal{V}^{\mathrm{COMPR}} = (\mathcal{S}^{\mathrm{COMPR}}, \mathcal{D}^{\mathrm{COMPR}}) = \mathsf{Compress}_\lambda(\mathcal{V})$
  3. Return $\mathcal{D}^{\mathrm{COMPR}}(n, x, y, a, b)$

  If it has not stopped after $(\Delta n)^\Delta$ steps, reject

Claim: $\mathcal{F}$ halts on all inputs and the description of $\mathcal{F}$ can be computed in time $\mathrm{poly}(|\mathcal{M}|, \log \lambda, \log \Delta)$

Notation: $\mathcal{M} \equiv \mathcal{M}'$ when they compute the same function

Theorem (Applying the Kleene-Roger fixed point theorem to $\mathcal{F}$)

Because $\mathcal{F}$ halts on all inputs, there exists a TM $\mathcal{D}^{\mathrm{HALT}}$ such that $\mathcal{D}^{\mathrm{HALT}} \equiv \mathcal{F}(\mathcal{D}^{\mathrm{HALT}})$
In addition, there is a Turing machine $\mathsf{ComputeFP}_k$ such that $\mathsf{ComputeFP}_k(\overline{\mathcal{F}}) = \overline{\mathcal{D}^{\mathrm{HALT}}}$
Moreover, $\mathcal{D}^{\mathrm{HALT}}(x)$ runs in time $\mathrm{poly}(|\mathcal{F}|, \mathsf{TIME}_{\mathcal{F},\mathcal{M}}, \mathsf{TIME}_{\mathcal{F}(\mathcal{D}^{\mathrm{HALT}}),x})$

Define $\mathcal{V} = (\mathcal{S}^{\mathrm{COMPR}}, \mathcal{D}^{\mathrm{HALT}})$ be a normal form verifier. Then it satisfies the following properties:

- For any n, if $\mathcal{M}$ halts in n steps, then $\mathrm{val}^*(\mathcal{V}_n) = 1$
- For any n, if $\mathcal{M}$ does not halt in n steps then the decision predicate for $\mathcal{V}_n$ is defined as $\mathcal{D}^{\mathrm{COMPR}}(n, x, y, a, b)$
  $\implies \mathrm{val}^*(\mathcal{V}_n) = \mathrm{val}^*(\mathcal{V}_n^{\mathrm{COMPR}})$ and $\mathscr{E}(\mathcal{V}_n, \frac{1}{2}) = \mathscr{E}(\mathcal{V}_n^{\mathrm{COMPR}}, \frac{1}{2})$

Putting things together

Theorem (Game value at least as hard as halting)

For all Turing machines $\mathcal{M}$, there exists a game $\mathfrak{G}_{\mathcal{M}}$ such that

- *If $\mathcal{M}$ halts on empty tape, then* $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = 1$
- *If $\mathcal{M}$ does not halt on empty tape, then* $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) \leq \frac{1}{2}$

Moreover, a description of the game $\mathfrak{G}_{\mathcal{M}}$ can be computed in polynomial time in the size of the description of $\mathcal{M}$.

- Given $\mathcal{M}$ compute appropriately large enough λ, Δ (to guarantee that later $\mathcal{V}$ is λ-bounded and $\mathcal{F}(\mathcal{D})$ does not exceed the time bound)
- Construct $\mathcal{V}$ such that $\mathcal{D} \equiv \mathcal{F}(\mathcal{D})$
- The game $\mathfrak{G}_{\mathcal{M}}$ will be defined as the $\mathcal{V}_{n_0}$
- If $\mathcal{M}$ halts after T steps then for $n \geq T$, $\mathrm{val}^*(\mathcal{V}_n) = 1$ (all questions and answers win!)
  For $n_0 \leq n < T \leq 2^n$, then $\mathcal{D}(n, x, y, a, b) = \mathcal{D}^{\mathrm{COMPR}}(n, x, y, a, b)$
  but we know that $\mathrm{val}^*(\mathcal{V}_{2^n}) = 1$, thus $\mathrm{val}^*(\mathcal{V}_n^{\mathrm{COMPR}}) = \mathrm{val}^*(\mathcal{V}_n) = 1$
  In general, repeat this inductively
- If $\mathcal{M}$ does not halt, we have for $n \geq n_0$
  $\mathscr{E}(\mathcal{V}_n, \frac{1}{2}) = \mathscr{E}(\mathcal{V}_n^{\mathrm{COMPR}}, \frac{1}{2}) \geq \mathscr{E}(\mathcal{V}_{2^n}, \frac{1}{2})$
  Repeating, $\mathscr{E}(\mathcal{V}_n, \frac{1}{2}) \geq \mathscr{E}(\mathcal{V}_{2^{2^{\cdots 2^n}}}, \frac{1}{2}) \geq \frac{1}{2} 2^{\lambda 2^{\lambda 2^{\cdots 2^n}}}$
  $\mathscr{E}(\mathcal{V}_n, \frac{1}{2}) = +\infty \Leftrightarrow \mathrm{val}^*(\mathcal{V}_n) \leq \frac{1}{2}$

Suggestions for future talks

- Self testing and nonlocal games
- PCP theorem
- Quantum low-degree test
- Putting things together