Compression of Nonlocal Games

Sajjad Nezhadi

Hanoon Mousavi  Henry Yuen
Nonlocal Games

\[ G = (Q, A, D) \]

- \( x \in Q \): Sampled questions
- \( a \in A \): Possible responses
- \( D(x, y, a, b) \): win condition
Null leads Games

\[
W(G) = \text{max win probability over classical/non-entangled Strategies}
\]

\[
W^*(G) = \text{max win probability using entangled Strategies}
\]

\[G = (Q, A, D)\]

\[X \subseteq Q \text{ Sampled questions} \]

\[A \subseteq \text{Possible responses} \]

\[D(x,y,q,b) \text{ win condition} \]
Nonlocal Games

\[ W(G) = \max \text{ win probability over classical/non-entangled Strategies} \]

\[ W^*(G) = \max \text{ win probability using entangled Strategies} \]

- Nonlocal games model interactive proofs with multiple provers
- Used for experimental proofs of quantumness
- Widely used in Q-cryptography

\( G = (Q, A, D) \)

\( x, j \in Q \), sampled questions

\( a, b \in A \), possible responses

\( D(x,y,a,b) \), win condition
Magic Square Game

\[ Q_A = \begin{cases} 
  x_1 + x_2 + x_3 = 0 \\
  x_4 + x_5 + x_6 = 0 \\
  x_7 + x_8 + x_9 = 0 \\
  x_1 + x_4 + x_7 = 0 \\
  x_2 + x_5 + x_8 = 0 \\
  x_3 + x_6 + x_9 = 1 
\end{cases} \]

\[ Q_B = \{ x_1, \ldots, x_9 \} \]

\[ A = \{ 0, 1 \} \]
Magic Square Game

\[ Q_A = \begin{cases} 
\frac{x_1 x_5 x_3}{1} \\
\frac{x_4 x_5 x_6}{1} \\
\frac{x_7 x_8 x_9}{1} \\
\frac{x_3 x_6 x_9}{-1}
\end{cases} \]

\[ Q_B = \{ x_1, \ldots, x_9 \} \]

A = \{ +1, -1 \}

\[ w(MS) = \frac{17}{18} \]

\[ w^*(MS) = 1 \]

The equations are not simultaneously satisfiable

The equations have an operator solution
Complexity of $w^*(6)$

How hard is it to decide if $w^*(6) = 1$ given a nonlocal game $G$?

Alternatively, how powerful are entangled multiprover interactive protocols?
Complexity of $\omega^*(6)$

How hard is it to decide if $\omega^*(6) = 1$ given a nonlocal game $G$?

The promise problem $\omega^*(6) = 1$ or $\omega^*(6) \leq \frac{1}{2}$ was shown to be equivalent to the halting problem in the $\text{MIP}^* = \text{RE}$ paper of JNvWY.
Complexity of $\mathbb{w}^*(6)$

How hard is it to decide if $\mathbb{w}^*(6) = 1$ given a nonlocal game $G$?

The promise problem $\mathbb{w}^*(6) = 1$ or $\mathbb{w}^*(6) \leq \frac{1}{2}$ was shown to be equivalent to the halting problem in the MIP$^* = \mathsf{RE}$ paper of JNWWY.

We showed exactly deciding if $\mathbb{w}^*(6) = 1$ is even more undecidable and equivalent to the universal halting problem.
Complexity of $w^*(6)$

How hard is it to decide if $w^*(6) = 1$ given a nonlocal game $G$?

The promise problem $w^*(6) = 1$ or $w^*(6) \leq 1/2$ was shown to be equivalent to the halting problem in the MIP* = RE paper of JNvWvY.

We showed exactly deciding if $w^*(6) = 1$ is even more undecidable and equivalent to the universal halting problem.

Both these results use a technique known as iterated compression.
Computability Recap

Halting Problem: Decide if $T(x)$ halts for a fixed $x$.

RE-complete
Computability Recap

Halting Problem: Decide if $T(x)$ halts for a fixed $x$.

RE-complete

Non-Halting Problem: Decide if $T(x)$ runs indefinitely for fixed $x$.

coRE-complete
Computability Recap

Halting Problem: Decide if $T(x)$ halts for a fixed $x$.

$\uparrow$

RE-complete

Non-Halting Problem: Decide if $T(x)$ runs indefinitely for fixed $x$.

$\uparrow$

coRE-complete

Universal Halting Problem: Decide if $T(x)$ halts for every input $x$.

$\uparrow$

$\Pi_2$-complete
Computability Recap

**Halting Problem:** Decide if \( T(x) \) halts for a fixed \( x \).

RE-complete

**Non Halting Problem:** Decide if \( T(x) \) runs indefinitely for fixed \( x \).

\( \neg \) coRE-complete

**Universal Halting Problem:** Decide if \( T(x) \) halts for every input \( x \).

\( \neg \Pi_2 \) - Complete
Compression

\[
\begin{align*}
\# \text{Questions} & \quad N \quad \rightarrow \quad \log(N) \\
\# \text{Responses} & \quad N \quad \rightarrow \quad \log(N) \\
\text{Verifier Runtime} & \quad \text{poly}(n) \quad \rightarrow \quad \text{polylog}(N)
\end{align*}
\]
Compression

\[ \{ G_n \} \rightarrow \{ G'_n \} \]

- # Questions: \( N \rightarrow \log(N) \)
- # Responses: \( N \rightarrow \log(N) \)
- Verify Runtime: \( \text{poly}(n) \rightarrow \text{polylog}(N) \)

Related quantum values:

- \( w^*(6n') \geq \frac{1}{2} + \frac{1}{2} w^*(6n) \)
- \( w^*(6n)<1 \Rightarrow w^*(6n')<1 \)
$\forall n. \omega^*(6n) = 1 \iff \omega^*(G^\text{super}) = 1$
Super Compression

All. $\omega^*(6m) = 1 \iff \omega^*(G^{Sup}) = 1$

Reduction from Non-Halting.
Super Compression

\[ \forall n. \, \psi^*(6n) = 1 \iff \psi^*(G^{n+2}) = 1 \]

Reduction from Non-Halting.

Verifier runs \( T(x) \) for \( n \) steps and automatically makes players win if it does not halt.

O/w. makes players lose
Reduction from Non-Halting.

On verifier runs $T(x)$ for $n$ steps and automatically makes players win if it does not halt.

O/w. makes players lose

$T(x)$ runs forever $\iff$ $w^*(6n)=1 \ \forall n$. 

$\forall n. \ w^*(6n) = 1 \iff w^*(G^{sup}) = 1$
Super Compression

Reduction from Non-Halting.

On verifier runs $T(x)$ for $n$ steps and automatically makes players win if does not halt.

O/w. makes players lose

$T(x)$ runs forever $\iff$ $w^*(6n)=1 \ \forall n.$

Super Compress $\{6n\}$ to $6^*$

$\forall n. \ w^*(6n)=1 \iff w^*(6^*6n)=1$
Super Compression

Reduction from Non-Halting.

On verifier runs \( T(x) \) for \( n \) steps and automatically makes player win if does not halt.

O/w. makes players lose.

\( T(x) \) runs forever \( \iff \) \( w^*(6n) = 1 \) \( \forall n \).

Super Compress \( \{ 6n \} \) to \( 6^* \).

Then \( T(x) \) runs forever \( \iff \) \( w^*(6^*) = 1 \).

\( \forall n \). \( w^*(6n) = 1 \iff w^*(G^{Super}) = 1 \).
Super Compression

Reduction from Universal Halting.

∀n. w*(6n) = 1 ⇔ w*(G^{sup}) = 1
Super Compression

\[ \forall n. \ w^*(6n) = 1 \iff w^*(G^{super}) = 1 \]

Reduction from Universal Halting.

A verifier uses MIP* = RE reduction to obtain a game that decides if \( T(Bin(n)) \) halts.

Then proceeds to play according to it.
Super Compression

Reduction from Universal Halting.
On verifier uses $\mathsf{MIP^*} = \mathsf{RE}$ reduction to obtain game that decides if $T(\text{Bin}(n))$ Halts.
Then proceeds to play according to it.

$T(x)$ Halts for every $x$
$\iff \omega^*(G_x) = 1 \forall n.$

$\forall n. \omega^*(6n) = 1 \iff \omega^*(G^{super}) = 1.$
Super Compression

Reduction from Universal Halting.

A 6n verifier uses $\mathrm{MIP^*} = \mathrm{RE}$ reduction to obtain a game that decides if $T(\text{Bin}(n))$ Halts.

Then proceeds to play according to it.

$T(x)$ Halts for every $x$

$\iff w^*(G_n) = 1 \quad \forall n.$

Super Compress $\{6n\}$ to $G^*$

$\forall n. \; w^*(6n) = 1 \iff w^*(G^{\text{Super}}) = 1$
Super Compression

Reduction from Universal Halting.

A verifier uses $\text{MIP}^* = \text{RE}$ reduction to obtain a game that decides if $T(\text{Bin}(n))$ halts.

Then proceeds to play according to it.

$T(x)$ halts for every $x$ if

$\forall n. \quad \omega^*(6^n) = 1 \iff \omega^*(G^{\text{super}}) = 1$

Then $T(x)$ halts on every $x$ if

$\forall n. \quad \omega^*(6^#) = 1$
Iterated Compression

\{G_n\} : \\
\{H_n\} : \\
\{H_{n+1}\} : \\
\ldots

\vcenter{\scaledbox{\includegraphics[width=\textwidth]{image.png}}}

\vcenter{\includegraphics[width=\textwidth]{image.png}}
Iterated Compression

\[ \{G_n\} : \]

Family we wish to SuperCompress

\[ \{H_n\} : \]

New family we define such that \( G^* = H_1 \)

\[ \{H_n\} : \]

Compression of \( \{H_n\} \) family
Iterated Compression

\{G_n\} : \{H_n\} : \{H_{n+1}\} \\
\ldots

p = \frac{1}{2}
Iterated Compression

\{G_n\} : \rightarrow \{H_n\} : p^{\frac{\sqrt{2}}{4}} \quad \rightarrow \quad \{H_n\} : p^{\frac{\sqrt{2}}{4}} \quad \rightarrow \quad \{G_n\} : p^{\frac{\sqrt{2}}{4}}
Iterated Compression

Claim. \( w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n. \)
Claim:  $w^*(H_n) = 1 \iff w^*(G_n) = 1 \forall n$.

$H_n$:  
- $p = \frac{1}{2}$ play $G_n$
- $p = \frac{1}{2}$ play $H_{n+1}$

Compression:
- $w^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)$
- $w^*(H_n) < 1 \Rightarrow w^*(H_n^{comp}) < 1$
Claim: \( \omega^*(H_1) = 1 \iff \omega^*(G_n) = 1 \ \forall n. \)

If \( \omega^*(G_n) = 1 \ \forall n \)

\[ \begin{align*}
H_n: & \\
& \cdot p = \frac{1}{2} \text{ play } G_n \\
& \cdot p = \frac{1}{2} \text{ play } H_{n+1} \\
\end{align*} \]

Compression:
\[ \begin{align*}
& \cdot \omega^*(H_n^{\text{comp}}) \geq \frac{1}{2} + \frac{1}{2} \omega^*(H_n) \\
& \cdot \omega^*(H_n) < 1 \implies \omega^*(H_n^{\text{comp}}) < 1
\end{align*} \]
Claim: $w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n$.

If $w^*(G_n) = 1 \ \forall n$

$\implies w^*(H_n) = \frac{1}{2} + \frac{1}{2} w^*(H_{n+1}) \quad [\text{Def. } H_n]$

Hn:
- $p = \frac{1}{2}$ play $G_n$
- $p = \frac{1}{2}$ play $H_{n+1}$

Compression:
- $w^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)$
- $w^*(H_n) < 1 \implies w^*(H_n^{comp}) < 1$
Claim: \( w^*(H_n) = 1 \iff w^*(G_n) = 1 \ \forall n \).

If \( w^*(G_n) = 1 \ \forall n \)

\[ \Rightarrow w^*(H_n) = \frac{1}{2} + \frac{1}{2} w^*(H_{n+1}) \quad [\text{Def. } H_n] \]

\[ \Rightarrow w^*(H_n) \geq \frac{3}{4} + \frac{1}{2} w^*(H_{n+1}) \quad [\text{Comp}] \]

\[ H_n: \]
- \( p = \frac{1}{2} \) play \( G_n \)
- \( p = \frac{1}{2} \) play \( H_{n+1} \)

Compression:
- \( w^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n) \)
- \( w^*(H_n) < 1 \Rightarrow w^*(H_n^{comp}) < 1 \)
Claim: \( \omega^*(H_1) = 1 \iff \omega^*(G_n) = 1 \ \forall n \).

If \( \omega^*(G_n) = 1 \ \forall n \)

\[ \Rightarrow \omega^*(H_n) = \frac{1}{2} + \frac{1}{2} \omega^*(H_{n+1}) \quad \text{[Def. } H_n \text{]} \]

\[ \Rightarrow \omega^*(H_n) \geq \frac{3}{4} + \frac{1}{4} \omega^*(H_{n+1}) \quad \text{[Comp]} \]

\[ \vdots \]

\[ \Rightarrow \omega^*(H_1) \geq 1 - \lim_{n \to \infty} \frac{1}{4^n} (1 + \omega^*(H_n)) \]

\[ = 1 ! \]

\text{Hn:}
- \( p = \frac{1}{2} \) play \( G_n \)
- \( p = \frac{1}{2} \) play \( H_{n+1} \)

\text{Compression:}
- \( \omega^*(H_{n+1}) \geq \frac{1}{2} + \frac{1}{2} \omega^*(H_n) \)
- \( \omega^*(H_n) < 1 \Rightarrow \omega^*(H_{n+1}) < 1 \)
Claim: $\omega^*(H_1) = 1 \iff \omega^*(G_n) = 1 \forall n$.

If $\omega^*(G_k) < 1$ for some $k$.

**Hn:**
- $p = \frac{1}{2}$ play $G_n$
- $p = \frac{1}{2}$ play $\mathcal{H}_{n+1}$

**Compression:**
- $\omega^*(H_n^{\text{comp}}) \geq \frac{1}{2} + \frac{1}{2} \omega^*(H_n)$
- $\omega^*(H_n) < 1 \implies \omega^*(H_n^{\text{comp}}) < 1$
Claim: $w^*(H_1) = 1 \iff w^*(G_n) = 1 \forall n$.

If $w^*(G_k) < 1$ for some $k$.

$$
\implies w^*(H_k) = \frac{1}{2} w^*(H_{\lambda,11}) - \frac{1}{2} w^*(G_k) \quad [\text{Def. } H_n]
$$

$$< 1$$

Hn:
- $p = \frac{1}{2}$ play $G_n$
- $p = \frac{1}{2}$ play $H_{n+1}$

Compression:
- $w^*(H_{n+1}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)
- w^*(H_n) < 1 \implies w^*(H_{n+1}) < 1$
**Claim:** $w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n$.

If $w^*(G_k) < 1$ for some $k$.

$$\Rightarrow w^*(H_k) = \frac{1}{2} w^*(H_{comp}^{k+1}) - \frac{1}{2} w^*(G_k) \quad [\text{Def. } H_n]$$

$$< 1$$

$$\Rightarrow w^*(H_{k+1}) < 1 \quad [\text{Comp}]$$

**Hn:**
- $p = \frac{1}{2}$ play $G_n$
- $p = \frac{1}{2}$ play $H_{n+1}$

**Compression:**
- $w^*(H_{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)$
- $w^*(H_n) < 1 \Rightarrow w^*(H_{comp}) < 1$
Claim: \( w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n. \)

If \( w^*(G_k) < 1 \) for some \( k. \)

\[
\implies w^*(H_k) = \frac{1}{2} w^*(H_k^{\text{comp}}) - \frac{1}{2} w^*(G_k) \quad \text{[Def. \( H_n \)]}
\]

\[
< 1
\]

\[
\implies w^*(H_k^{\text{comp}}) < 1 \quad \text{[Comp]}
\]

\[
\implies w^*(H_{k-1}) < 1 \quad \text{[Def. \( H_n \)]}
\]

\[
H_n:\quad \begin{align*}
P &= \frac{1}{2} \text{ play } G_n \\
P &= \frac{1}{2} \text{ play } H_{n+1}
\end{align*}
\]

Compression:

\[
\begin{align*}
w^*(H_k^{\text{comp}}) &\geq \frac{1}{2} + \frac{1}{2} w^*(H_n) \\
w^*(H_n) < 1 &\implies w^*(H_k^{\text{comp}}) < 1
\end{align*}
\]
Claim: $w^*(H_n) = 1 \iff w^*(G_n) = 1 \forall n.$

If $w^*(G_k) < 1$ for some $k$.

$$\implies w^*(H_k) = \frac{1}{2} w^*(H_{k+1}^\text{comp}) - \frac{1}{2} w^*(G_k) \quad [\text{Def. } H_n]$$

$$< 1$$

$$\implies w^*(H_k^\text{comp}) < 1 \quad [\text{Comp}]$$

$$\implies w^*(H_{k-1}) < 1 \quad [\text{Def. } H_n]$$

$$\vdots$$

$$\implies w^*(H_1) < 1!$$
Recap

We have used **Compression** to map a family of games \( \{ G_n \} \) to a single game \( G^* \) so that \( \text{W}^*(G^*) = 1 \Rightarrow \text{W}^*(G_n) = 1 \ \forall n. \)

Using this Supercompression map we immediately get a reduction from **non-Halting** to deciding \( \text{W}^*(G) = 1. \)

And using \( \text{MIP}^* = \text{RE} \) we can improve this to a reduction from **Universal Halting**.
How to Compress

Answer Reduction

Delegate deciding if the players won to the players and ask them for a short proof that they won instead. [Think PCP]

Question Reduction
How to Compress

Answer Reduction
Deligate deciding if the players won to the players and ask them for a short proof that they won instead [Think PCP]

Question Reduction
Ask the players to sample their own questions.
To verify the questions were sampled honestly play a game with appropriate rigidity properties [Think Randomness expansion]
How to Compress

Answer Reduction

Delegate deciding if the players won to the players and ask them for a short proof that they won instead [Think PCP]

Question Reduction ← Quantum enters

Ask the players to sample their own questions. To verify the questions were sampled honestly play a game with appropriate rigidity properties [Think Randomness expansion]
Any quantum strategy winning the MS game must be sharing two EPR entangled states and measuring them in a particular bases. Generating two uniformly sampled bits.
Rigidity

Any quantum strategy winning the MS game must be sharing two EPR entangled states and measuring them in a particular bases. Generating two uniformly sampled bits.

We want a similar phenomena which is more efficient i.e. bits sampled as questions exponentially smaller than bits forced to be generated as responses.
Thank you