Compiled Nonlocal Games

Sum of Squares Optimization Meets Cryptography?

Anand Natarajan & Tina Zhang  arXiv:2303.01545
Nonlocal Games

Invented by John Bell to test quantum mechanics
Nonlocal Games

Invented by John Bell to test quantum mechanics

Referee (classical)

Alice

Bob
Nonlocal Games

Invented by John Bell to test quantum mechanics

Referee (classical)

Alice

Bob
Nonlocal Games

Invented by John Bell to test quantum mechanics

Referee (classical)

\[ P_{\text{min}} = \frac{Pr_{\text{a,ij}}}{Pr_{\text{b,ij}}} \]

Answers

\( a, b \) are "commit" for questions \( i, j \)
Nonlocal Games

Invented by John Bell to test quantum mechanics

Referee (classical)

\[ P_{\text{win}} = \begin{bmatrix} \text{Answers} \\ a, b \end{bmatrix} \]

\[ a, b \text{ are } \text{ "commit" for questions } a, b \]

In general

\[ P_{\text{win}} \leq \text{quantum } P_{\text{win}} \]

Alice

Bob
The CHSH Game

\[ i,j \in \{0,13\} \]
\[ a,b \in \{3 \pm 13\} \]

Win if \( ab = (-1)^{s_{ij}} \)

<table>
<thead>
<tr>
<th>i ( \times ) j</th>
<th>( ab )</th>
<th>( s_{ij} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 ( \times ) 0</td>
<td>0 ( \times ) 0</td>
<td>0 ( \times ) 0</td>
</tr>
<tr>
<td>0 ( \times ) 1</td>
<td>1 ( \times ) 1</td>
<td>0 ( \times ) 0</td>
</tr>
<tr>
<td>1 ( \times ) 0</td>
<td>1 ( \times ) 1</td>
<td>0 ( \times ) 0</td>
</tr>
<tr>
<td>1 ( \times ) 1</td>
<td>-1 ( \times ) -1</td>
<td>1 ( \times ) 1</td>
</tr>
</tbody>
</table>
The CHSH Game

\[ i,j \in \{0,13\} \]
\[ a, b \in \{3 \pm 13\} \]

Win if \( ab = (-1)^{s_{ij}} \)
The CHSH Game

\[ P_{\text{win}} = \frac{1}{2} + \frac{1}{2} \beta \]

\[ \beta = \max_{\text{classical}} \left\{ E(\xi) \right\} \quad \text{a}_{ij} \cdot b_{ij} \]

st. \quad \forall i \; a_i^2 = 1 \quad \forall j \; b_j^2 = 1
The CHSH Game

\[ P_{\text{win}} = \frac{1}{2} + \frac{1}{2} \beta \]

\[ \beta = \max \{ \mathbb{E} (\xi | a_i, b_j) \} \]

\text{st. } \forall i \ a_i^2 = 1
\quad \forall j \ b_j^2 = 1

\[ \beta_{\text{classical}} = \frac{1}{2} \]

Set \( a_0 = a_1 = 1 \)
\quad \( b_0 = b_1 = 1 \)

\implies P_{\text{win}} = \frac{3}{4}
The CHSH Game

\[ P_{\text{win}} = \frac{1}{2} + \frac{1}{2} \beta \]

Quantum

\[ \beta = \max_{A_i, B_j, \rho} \left\{ E(\psi) + tr[\rho \left( A_i B_j \right)] \right\} \]

subject to \( \rho \leq 0, \rho^T = 1 \)

\[ \forall i, A_i^2 = I \]

\[ \forall j, B_j^2 = I \]

\[ \forall i, j \text{ } A_i B_j = B_j A_i \]
The CHSH Game

\[ P_{\text{min}} = \frac{1}{2} + \frac{1}{2} \beta \]

\[ \beta = \max_{A_i B_j} \left[ E(S_i) + \epsilon \left[ A_i B_j P \right] \right] \]

\text{subject to:} \quad \epsilon \leq 0, \quad \epsilon + P = 1

\forall i, \quad A_i^2 = I

\forall j, \quad B_j^2 = I

\forall i,j, \quad A_i B_j = B_j A_i

\beta = \frac{1}{2} \sqrt{2} \quad \text{quantum}

\beta \geq \beta_{\text{classical}}
The CHSH Game

$$P_{\text{win}} = \frac{1}{2} + \frac{1}{2} \beta$$

$\beta = \max_{\tilde{x}, \tilde{y}, p} \left\{ E(\tilde{x}) + \sum_{i,j} T_{ij} \left[ A_i \otimes B_j \otimes p \right] \right\}$

s.t. $p \leq 0$, $+p = 1$

$\forall i$, $A_i^2 = I$

$\forall j$, $B_j^2 = I$

$\forall i,j$, $A_i \otimes B_j = B_j \otimes A_i$

$$\beta = \frac{1}{2} \sqrt{2}$$

$$P_{\text{win}} = 0.85 > \frac{3}{4}$$
The CHSH Game

- quantum > classical demonstrated in lab [2022 Nobel Prize]

Q. optimizer is "rigid"

\[ \beta^Q(\mathbf{A}, \mathbf{B}) \times \frac{1}{\sqrt{2}} \Rightarrow A_0A_1 \equiv -A_1A_0 \]

Anticommutation \( \Rightarrow \) "complementary in physics measurements"
The CHSH Game

Q. optimizer is “rigid”

\[ \beta^Q(A, B) \propto \frac{1}{2} \sqrt{\alpha} \Rightarrow \begin{align*}
    A_0A_1 &= -A_1A_0 \\
    B_0B_1 &= -B_1B_0
\end{align*} \]

Anticommutation \(\Rightarrow\) “complementary measurements” in physics

\[ \Rightarrow \text{Using CHSH, can build protocols to test quantum computers “gate by gate”} \]

[RU'13]
Drawbacks of nonlocal games
Drawbacks of nonlocal games

- Non-communication between players is essential.
  - a must only depend on i
  - b must only depend on j
Drawbacks of nonlocal games

- Non-communication between players is essential

  \[ a \text{ must only depend on } i \]

  \[ b \text{ must only depend on } j \]

Quantum: \( A_i \) and \( B_j \) must be commuting matrices
Drawbacks of nonlocal games

- Non-communication between players is essential.
  
  \[ a \text{ must only depend on } i \]
  
  \[ b \text{ must only depend on } j \]

Quantum: \( A_i \) and \( B_j \) must be commuting matrices.

Experimentally very difficult to realize!
Cryptographic Compilers

Idea: Use cryptography so one player can "simulate" 2 separated players.

[Long history in crypto, e.g. Kilian '92, BMW'98, KRR'14,.....]
Cryptographic compilers

- Idea: Use cryptography so one player can "simulate" 2 separated players

[KLKVY'22]
Cryptographic compilers

round 1

Enc(i)

Enc(a)

round 2

b

[KLVY'22]: $P_{\text{min}}^{\text{compiled}} \leq P_{\text{min}}^{\text{nonlocal}} + \text{negl.}$
Cryptographic compilers

\[ A \xrightarrow{\text{round 1}} B \xrightarrow{\text{round 2}} \]

\[ \text{Enc}(i) \xrightarrow{\text{round 1}} \text{Enc}(a) \xrightarrow{\text{round 2}} b \]

[KLVY'22]: \( P_{\text{Q compile}} \leq P_{\text{Q nonlocal}} + \text{negl.} \)
Cryptographic compilers

### Compilers: CHSH

<table>
<thead>
<tr>
<th></th>
<th>Classical</th>
<th>Quantum</th>
</tr>
</thead>
<tbody>
<tr>
<td>nonlocal</td>
<td>$3/4$</td>
<td>$0.85$</td>
</tr>
<tr>
<td>compiled</td>
<td>$3/4 + \text{neg!}$</td>
<td>???</td>
</tr>
</tbody>
</table>
Our results

<table>
<thead>
<tr>
<th></th>
<th>Classical</th>
<th>Quantum</th>
</tr>
</thead>
<tbody>
<tr>
<td>nonlocal</td>
<td>$\frac{3}{4}$</td>
<td>$0.85 \left( \frac{1}{3} + \frac{\sqrt{2}}{4} \right)$</td>
</tr>
<tr>
<td>compiled</td>
<td>$\frac{3}{4} + \text{neg!}$</td>
<td>$0.85 + \text{neg!} \left( \frac{1}{2} + \frac{\sqrt{2}}{4} + \text{neg!} \right)$</td>
</tr>
</tbody>
</table>
Our results: rigidity

<table>
<thead>
<tr>
<th>Nonlocal</th>
<th>Classical</th>
<th>Quantum</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/4</td>
<td>3/4 + neg!</td>
<td>0.85 (\left(\frac{1}{2} + \frac{\sqrt{2}}{4}\right))</td>
</tr>
</tbody>
</table>

Any strategy that is near optimal must have

\[B_0B_1 x = -B_1 B_0\]
Our results: delegation

<table>
<thead>
<tr>
<th>nonlocal</th>
<th>classical</th>
<th>quantum</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/4</td>
<td>3/4 + neg1</td>
<td>0.85 ((\frac{1}{3} + \frac{\sqrt{2}}{4}))</td>
</tr>
</tbody>
</table>

0.85 + neg1

\((\frac{1}{2} + \frac{\sqrt{2}}{4} + \text{neg}!\))

A delegation scheme for poly-time quantum computation w/ classical client (assuming quantum fully homomorphic encryption \(\in\ \text{LWE \ [Mahadev'17]}\))
Our results: delegation

<table>
<thead>
<tr>
<th>nonlocal</th>
<th>classical</th>
<th>3/4</th>
<th>quantum</th>
<th>0.85 ($\frac{1}{3} + \frac{\sqrt{2}}{4}$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>compiled</td>
<td>compiled</td>
<td>3/4 + neg!</td>
<td></td>
<td>0.85 + neg! ($\frac{1}{2} + \frac{\sqrt{2}}{4} + \text{neg!}$)</td>
</tr>
</tbody>
</table>

A delegation scheme for poly-time quantum computation w/ classical client

(assuming quantum fully homomorphic encryption $\in$ LWE [Mahadev '18])

Matches [Mahadev '18] by new techniques
Techniques: outline

1) Prove $\beta^2 \leq \frac{1}{2} \sqrt{2}$ in nonlocal until using noncommutative Sum-of-Squares

2) Modify this proof to show

$$\beta_{\text{compiled}}^2 \leq \frac{1}{2} \sqrt{2} + \text{negl}.$$
SOS for $\beta^q$

\[
\beta^q = \max \quad \text{tr} \quad \hat{G}(A, A_i, B, B_i)
\]

\[
\begin{bmatrix}
\mathbf{E}^{(-1)} \quad A_i \quad B_j \\
0 \quad I \quad A_i B_j
\end{bmatrix}
\]

s.t.

\[
A_i^2 = B_j^2 = I, \quad A_i B_j = B_j A_i
\]

\[
p \geq 0, \quad \text{tr} p = 1
\]
SOS for $\beta^Q$

$$\beta^Q = \max \quad \text{tr} \left[ \sum_{i,j} E(-1) A_i B_j \right]$$

s.t. \quad $A_i^2 = B_j^2 = I, A_i B_j = B_j A_i$ (*)

$p \geq 0$, $\text{tr} p = 1$

To show $\beta^Q \leq \frac{1}{2} \sqrt{2}$, suffices to show

$$\frac{1}{2} \sqrt{2} - G \geq 0 \quad \text{whenever \, (*) \, holds}$$
To show $\beta^q \leq \frac{1}{2} \sqrt{2}$ it suffices to show

$$\frac{1}{\sqrt{2}} \cdot \widehat{g} \geq 0 \quad \text{(4)}$$

and

$$\frac{1}{2} \cdot \sum_{A, B} -\widehat{g}(A, B) = \sum_k P_k(A, B)^+ P_k(A, B) \quad \text{mod (4)}$$

is

\text{sum of squares} \quad \text{(must be } \leq 0)
To show $\beta^2 \leq \frac{1}{2} \sqrt{2}$ suffices to show

\[
\frac{1}{2} \cdot \text{det}^{-1} G(A, B) = \sum_k p_k(A, B)^t p_k(A, B) \mod (4)
\]

Take

\[
P_1 = \left( A_0 - \frac{B_0 + B_1}{\sqrt{2}} \right)
\]

\[
P_2 = \left( A_1 - \frac{B_0 - B_1}{\sqrt{2}} \right)
\]
For $\beta^Q$, we have:

$$\beta^Q = \max \{ \mathbf{E} (-1)^{s_{ij}} A_i B_j \}$$

subject to:

$$A_i^2 = B_j^2 = I, \quad A_i B_j = B_j A_i$$

and

$$p \geq 0, \quad p = 1$$

To show $\beta^Q \leq \frac{1}{2} \sqrt{2}$, it suffices to show:

$$\frac{1}{2} \cdot \frac{1}{\sqrt{2}} \sum k P_k^{(A,B)} = \sum k P_k^{(A,B)} P_k^{(A,B)} \mod (\#)$$

Take

$$P_1 \propto \left( A_0 - \frac{B_0 + B_1}{\sqrt{2}} \right)$$

and

$$P_2 \propto \left( A_1 - \frac{B_0 - B_1}{\sqrt{2}} \right)$$

rigidity

Near optimal strategies have

$$p_k \approx 0$$
SOS for $\beta^Q_{\text{compiled}}$

$$\beta^Q_{\text{compiled}} = \max tr \left[ \sum_{i=0}^{s} \sum_{j} (-1)^{s_j} A_i^{(a)} B_j A_i^{(a)} \rho \right]$$

s.t.

$$\forall i_j \sum_{a} A_i^{(a)+} A_i^{(a)} = I$$

$$\forall j B_j^2 = I$$

$$P \geq 0, \quad tr P = 1$$
SoS for $\beta_{\text{coupled}}^Q$ sequential quantum measurement

$$\beta_{\text{compiled}}^Q = \max \text{tr} \left[ \sum_i \sum_j (-1)^{s_{ij}} A_i^{(a)^*} B_j A_i^{(a)} \rho \right]$$

s.t.

\[ \forall i, \sum_a A_i^{(a)^*} A_i^{(a)} = I \]

\[ \forall j, B_j^2 = I \]

\[ \rho \geq 0, \text{ tr}\rho = 1 \]
SOS for $\beta_{\text{compiled}}$ quasileading

$$\beta_{\text{compiled}}^Q = \max \operatorname{tr}\left[ \sum_{\alpha} \mathbb{E} \left( -1 \right)^{s_{ij}} A_i^{(\alpha)} B_j A_i^{(\alpha)} \rho \right]$$

s.t.

$$\forall i, j \ni \sum_{\alpha} A_i^{(\alpha)^+} A_i^{(\alpha)} = I$$

$$\forall j \ni B_j^2 = I$$

A $\forall i, j$ A “efficient” $f(B)$ $\operatorname{tr}[\sum_{\alpha} A_i^{(\alpha)^{f(B)}} A_i^{(\alpha)} \rho] \approx_{\epsilon_{\text{tol}}} 0$

$p \geq 0$, $p = 1$
SoS for $\beta_{\text{compiled}}$

$$\beta_{\text{compiled}}^Q = \max \, \text{tr} \left[ \sum_a \sum_{i,j} (-1)^{i-j} A_i^{(a)} B_j A_i^{(a)\top} p \right]$$

s.t.

1. $\forall i, j \sum_a A_i^{(a)\top} A_i^{(a)} = I$
2. $\forall j \quad B_j^2 = I$

$A_{ij}, A_{ij} \sim \text{"efficient", } f(B)$

$s_{\text{no}} \left[ \sum_a A_i^{(a)\top} f(B) A_i^{(a)} p \right]_{a=0,1}$

$p \geq 0, \quad \text{tr} p = 1$
\[
S_0 S \quad \text{for} \quad \beta_{\text{compiled}}^Q
\]

\[
\beta_{\text{compiled}}^Q = \max \left\{ \mathrm{tr} \left[ \sum_a E^{-1} s_{ij} A_{ij}^{(a)} B_{ji} A_{ij}^{(a)} \rho \right] \right\}
\]

s.t.
\begin{align*}
\forall i, j : A_{ij}^{(a)\dagger} A_{ij}^{(a)} &= I \\
\forall j : B_{ji}^2 &= I
\end{align*}

\begin{quote}
"No measurement in round 2 can leak info about $i$ (since it is encrypted)"
\end{quote}

\[
\forall j, A, \text{ "efficient" } f(B)
\]

\[
\mathrm{tr} \left[ \sum_a A_{ij}^{(a)\dagger} f(B) A_{ij}^{(a)} \rho \right] \approx_{n_01}
\]

\[
\mathrm{tr} \left[ \sum_a A_{ij}^{(a)\dagger} f(B) A_{ij}^{(a)} \rho \right]
\]

\[
p \geq 0, \quad + p = 1
\]
\[ S_0 S \text{ for } \beta_{\text{coupled}} \]

\[ \beta_{\text{compiled}}^Q = \max \tr \left[ \sum_a \prod_j \left( I - A_i A_i^\dagger B_j A_i^\dagger \right) \right] \]

s.t.
\[ \forall j, \sum_a A_i A_i^\dagger A_i^\dagger = I \]
\[ \forall j, B_j^2 = I \]

\[ \text{efficiency } f(B) \]
\[ \forall i,j, A \] \[ \text{tr} \left[ \sum_a A_i A_i^\dagger f(B) A_i^\dagger \right] > 0 \]

\[ \text{tr} \left[ \sum_a A_i A_i^\dagger f(B) A_i^\dagger \right] \]

Can we show
\[ \frac{1}{2} \sqrt{2} - G_{\text{compiled}} \]
\[ = \sum p^p \]
\[ \text{mod } (\ast \ast) \]?
SOS for $\beta_{\text{compiled}}^a$

$$\beta_{\text{compiled}}^a = \max \text{tr} \left[ \sum_{i,j} (\mathds{1} - A_i^a B_j A_i^a \rho \right]$$

s.t.

$$\forall i, j \sum_a A_i^{a+} A_i^{a-} = \mathds{1}$$

$$\forall i, B_i^2 = \mathds{1}$$

$A_i^a$, $A$ "efficient" $\mathcal{f}(\Theta)$

$p \geq 0$, $+p = 1$

We show

$$\text{tr} \left[ \left( \frac{1}{2} \mathds{1} - \mathcal{G}_{\text{compiled}} \right) \rho \right] = \text{tr} \left[ \sum p^+ p \rho \right]$$

mod $(\# \#)$

which is sufficient!
Open questions

- What about other games?
  When is $P_{\text{win}}^{Q, \text{compiled}} \leq P_{\text{win}}^Q + \text{neg}!$?
Open questions

- What about other games?
  When is $P_{\text{win}}^{Q, \text{compil}} \leq P_{\text{win}}^Q + \text{neg}$?

- Our SoS manipulations are very specific to CHSH
  - can we "lift" all simple SoS proofs (e.g. degree-2 proofs)?
Open questions

- What about other games?

  - When is $P_{\text{win}}^{Q, \text{compiled}} \leq P_{\text{win}}^{Q} + \text{neg}$?

- Our SoS manipulations are very specific to CHSH
  - can we "lift" all simple SoS proofs (e.g. degree-2 proofs) ?

- Can the cryptographic requirements be relaxed? (Less than full QFT?)
Open questions

- Does quantum crypto give rise to interesting new non-commutative polynomial optimization problems?
Thank you!

arXiv: 2303.01545