# Exams

Omar Fawzi

ENS DE LYON

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Oct 28th, 2015

with Norm Beaudry, Frédéric Dupuis and Renato Renner

# Randomness for testing

Randomness used to test a property
(specific state, Bell violation,...)

- Many systems $Y_1 \ldots Y_n$
- Want: testing random subset enough to guarantee global property

# Randomness for testing

Randomness used to test a property
(specific state, Bell violation,...)

- Many systems $Y_1 \ldots Y_n$
- Want: testing random subset enough to guarantee global property

Another property we would like to test:

$$\boxed{\text{Has student } B \text{ learned the data } X_1 \ldots X_n\text{?}}$$

- Want: testing random subset enough to guarantee global learning

# Probabilistic model

Systems:

- Data: $X_1, \ldots, X_n \in \{0,1\}^n$
- Student memory: $B$ (could be classical or quantum)

Modeled by a joint distribution $P_{X_1 \ldots X_n B}$

# Probabilistic model

Systems:

- Data: $X_1, \ldots, X_n \in \{0,1\}^n$
- Student memory: $B$ (could be classical or quantum)

Modeled by a joint distribution $P_{X_1 \ldots X_n B}$

Test:

- Exam: $\vec{i} = (\vec{i}_1, \ldots, \vec{i}_k)$ with $\vec{i}_p \in \{1, \ldots, n\}$
- Given $B$ and $\vec{i}$, answer $A^{\vec{i}} = A^{\vec{i}}(B, \vec{i}) \in \{0,1\}^k$
- Grade given by $\mathsf{G}_k = \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{i}_p} = A_p^{\vec{i}}} = k - d_H(X_{\vec{i}}, A^{\vec{i}})$

Property we are testing: correlation between $B$ and $X_1 \ldots X_n$

# Probabilistic model

Systems:

- Data: $X_1, \ldots, X_n \in \{0,1\}^n$
- Student memory: $B$ (could be classical or quantum)

Modeled by a joint distribution $P_{X_1 \ldots X_n B}$

Test:

- Exam: $\vec{i} = (\vec{i}_1, \ldots, \vec{i}_k)$ with $\vec{i}_p \in \{1, \ldots, n\}$
- Given $B$ and $\vec{i}$, answer $A^{\vec{i}} = A^{\vec{i}}(B, \vec{i}) \in \{0,1\}^k$
- Grade given by $\mathsf{G}_k = \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{i}_p} = A^{\vec{i}}_p} = k - d_H(X_{\vec{i}}, A^{\vec{i}})$

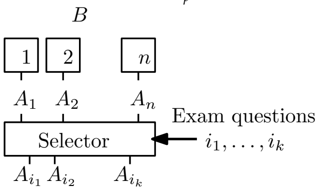
Property we are testing: correlation between $B$ and $X_1 \ldots X_n$

Think of the student as the adversary

# Exam strategies

**Notation:** Data: $X_1 \dots X_n \in \{0,1\}^n$ Exam: $\vec{i} = (\vec{i}_1, \dots, \vec{i}_k)$ with $\vec{i}_p \in \{1, \dots, n\}$
Student memory $B$ Answer $A^{\vec{i}} = A^{\vec{i}}(B, \vec{i}) \in \{0,1\}^k$ Grade $\mathsf{G}_k(A^{\vec{i}}) = \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{i}_p} = A^{\vec{i}}_p}$

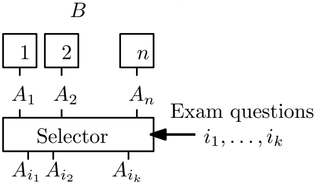
Special kind of strategy:
Simple strategies



# Exam strategies

**Notation:** Data: $X_1 \dots X_n \in \{0,1\}^n$ Exam: $\vec{i} = (\vec{i}_1, \dots, \vec{i}_k)$ with $\vec{i}_p \in \{1, \dots, n\}$
Student memory $B$ Answer $A^{\vec{i}} = A^{\vec{i}}(B, \vec{i}) \in \{0,1\}^k$ Grade $\mathsf{G}_k(A^{\vec{i}}) = \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{i}_p} = A_p^{\vec{i}}}$

Special kind of strategy:
Simple strategies

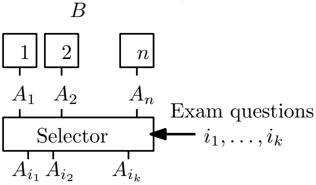


# Exam strategies

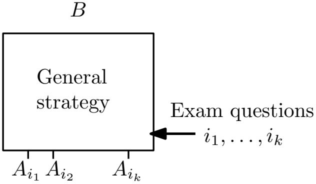
**Notation:** Data: $X_1 \dots X_n \in \{0,1\}^n$ Exam: $\vec{i} = (\vec{i}_1, \dots, \vec{i}_k)$ with $\vec{i}_p \in \{1, \dots, n\}$

Student memory $B$ Answer $A^{\vec{i}} = A^{\vec{i}}(B, \vec{i}) \in \{0,1\}^k$ Grade $\mathsf{G}_k(A^{\vec{i}}) = \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{i}_p} = A^{\vec{i}}_p}$

Special kind of strategy:
Simple strategies




General strategy
described by $\{A^{\vec{i}}\}_{\vec{i}}$




In general strategies, answer to question $i$ depends on context

# Desired statement

**Notation:** Data: $X_1, \ldots, X_n$ Exam: $\vec{i} = (\vec{i}_1, \ldots, \vec{i}_k)$ with $\vec{i}_p \in \{1, \ldots, n\}$

Student memory contains $B$ Answer $A^{\vec{i}} = A^{\vec{i}}(B, \vec{i}) \in \{0,1\}^k$ Grade $\mathsf{G}_k(A^{\vec{i}}) = \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{i}_p} = A^{\vec{i}}_p}$

# Desired statement

**Notation:** Data: $X_1, \ldots, X_n$ Exam: $\vec{i} = (\vec{i}_1, \ldots, \vec{i}_k)$ with $\vec{i}_p \in \{1, \ldots, n\}$

Student memory contains $B$ Answer $A^{\vec{i}} = A^{\vec{i}}(B, \vec{i}) \in \{0,1\}^k$ Grade $\mathsf{G}_k(A^{\vec{i}}) = \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{i}_p} = A^{\vec{i}}_p}$

Example: $X$ uniform on $\{0,1\}^n$ and

$$B = \begin{cases} X & \text{with prob. } 1/2 \\ 0 & \text{with prob. } 1/2 \end{cases}$$

# Desired statement

**Notation:** Data: $X_1, \ldots, X_n$ Exam: $\vec{i} = (\vec{i}_1, \ldots, \vec{i}_k)$ with $\vec{i}_p \in \{1, \ldots, n\}$

Student memory contains $B$ Answer $A^{\vec{i}} = A^{\vec{i}}(B, \vec{i}) \in \{0,1\}^k$ Grade $\mathsf{G}_k(A^{\vec{i}}) = \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{i}_p} = A_p^{\vec{i}}}$

Example: $X$ uniform on $\{0,1\}^n$ and

$$B = \begin{cases} X & \text{with prob. } 1/2 \\ 0 & \text{with prob. } 1/2 \end{cases}$$

$\rightarrow$ no absolute good/bad student

# Desired statement

**Notation:** Data: $X_1, \ldots, X_n$ Exam: $\vec{i} = (\vec{i}_1, \ldots, \vec{i}_k)$ with $\vec{i}_p \in \{1, \ldots, n\}$

Student memory contains $B$ Answer $A^{\vec{i}} = A^{\vec{i}}(B, \vec{i}) \in \{0,1\}^k$ Grade $\mathsf{G}_k(A^{\vec{i}}) = \sum_{p=1}^k \mathbf{1}_{X_{\vec{i}_p} = A_p^{\vec{i}}}$

Example: $X$ uniform on $\{0,1\}^n$ and

$$B = \begin{cases} X & \text{with prob. } 1/2 \\ 0 & \text{with prob. } 1/2 \end{cases}$$

$\rightarrow$ no absolute good/bad student

Property we are looking after:

memory $B$ allows answering many $X_1, \ldots, X_n$ correctly

**Theorem**

*For any $P_{X_1 \ldots X_n B}$ and any $\{A^{\vec{i}}\}_{\vec{i}}$, there exists an $\overline{A} = \overline{A}(B, \vec{i}, X_{\vec{i}}) \in \{0,1\}^n$ s.t.*

$$\mathbf{P}\left\{ \frac{\mathsf{G}_n(\overline{A})}{n} \leqslant \frac{\mathsf{G}_k(A^{\vec{i}})}{k} - \delta \right\} \leqslant e^{-\frac{\delta^2 k}{32}}$$

# Exam: simple strategies

**Notation:** Data: $X_1, \ldots, X_n$ Exam: $\vec{i} = (\vec{i}_1, \ldots, \vec{i}_k)$ with $\vec{i}_p \in \{1, \ldots, n\}$

Student memory contains $B$ Answer $A^{\vec{i}} = A^{\vec{i}}(B, \vec{i}) \in \{0,1\}^k$

For simple strategies, $A^{\vec{i}}_p = A_{\vec{i}_p}$ for some $A \in \{0,1\}^n$

We choose $\overline{A} = A$. Statement becomes

**Theorem**

*For any random variable $A = A_1 \ldots A_n$,*

$$\mathbf{P}_{\vec{i},X,A}\left\{\frac{1}{n}\sum_{\ell=1}^{n}\mathbf{1}_{X_\ell = A_\ell} \leqslant \frac{1}{k}\sum_{p=1}^{k}\mathbf{1}_{X_{\vec{i}_p} = A_{\vec{i}_p}} - \delta\right\} \leqslant e^{-\frac{\delta^2 k}{32}}$$

# Exam: simple strategies

**Notation:** Data: $X_1, \ldots, X_n$ Exam: $\vec{i} = (\vec{i}_1, \ldots, \vec{i}_k)$ with $\vec{i}_p \in \{1, \ldots, n\}$

Student memory contains $B$ Answer $A^{\vec{i}} = A^{\vec{i}}(B, \vec{i}) \in \{0,1\}^k$

For simple strategies, $A^{\vec{i}}_p = A_{\vec{i}_p}$ for some $A \in \{0,1\}^n$

We choose $\overline{A} = A$. Statement becomes

**Theorem**

*For any random variable $A = A_1 \ldots A_n$,*

$$\mathbf{P}_{\vec{i},X,A}\left\{\frac{1}{n}\sum_{\ell=1}^{n}\mathbf{1}_{X_\ell = A_\ell} \leqslant \frac{1}{k}\sum_{p=1}^{k}\mathbf{1}_{X_{\vec{i}_p} = A_{\vec{i}_p}} - \delta\right\} \leqslant e^{-\frac{\delta^2 k}{32}}$$

For fixed $X$ and $A$: standard bounds on hypergeometric distribution

# General case

**Theorem**

*For any strategy* $\{A^{\vec{i}}\}_{\vec{i}}$, *there exists an* $\overline{A} = \overline{A}(B, \vec{i}, X_{\vec{i}})$ *such that*

$$\mathbf{P}\left\{ \frac{\mathsf{G}_n(\overline{A})}{n} \leqslant \frac{\mathsf{G}_k(A^{\vec{i}})}{k} - \delta \right\} \leqslant e^{-\frac{\delta^2 k}{32}}$$

How to choose $\overline{A}$?

# General case

**Theorem**

*For any strategy* $\{A^{\vec{i}}\}_{\vec{i}}$*, there exists an* $\overline{A} = \overline{A}(B, \vec{i}, X_{\vec{i}})$ *such that*

$$\mathbf{P}\left\{\frac{\mathsf{G}_n(\overline{A})}{n} \leqslant \frac{\mathsf{G}_k(A^{\vec{i}})}{k} - \delta\right\} \leqslant e^{-\frac{\delta^2 k}{32}}$$

How to choose $\overline{A}$?

- Choose $\overline{A}_\ell = \textsc{maj}\{A^{\vec{j}}_\ell : \ell \in \vec{j}\}$

# General case

**Theorem**

*For any strategy* $\{A^{\vec{i}}\}_{\vec{i}}$*, there exists an* $\overline{A} = \overline{A}(B, \vec{i}, X_{\vec{i}})$ *such that*

$$\mathbf{P}\left\{\frac{\mathsf{G}_n(\overline{A})}{n} \leqslant \frac{\mathsf{G}_k(A^{\vec{i}})}{k} - \delta\right\} \leqslant e^{-\frac{\delta^2 k}{32}}$$

How to choose $\overline{A}$?

- Choose $\overline{A}_\ell = \textsc{maj}\{A^{\vec{j}}_\ell : \ell \in \vec{j}\}$
  does not work, have to use $\vec{i}$

# General case

## Theorem

*For any strategy* $\{A^{\vec{i}}\}_{\vec{i}}$*, there exists an* $\overline{A} = \overline{A}(B, \vec{i}, X_{\vec{i}})$ *such that*

$$\mathbf{P}\left\{\frac{\mathsf{G}_n(\overline{A})}{n} \leqslant \frac{\mathsf{G}_k(A^{\vec{i}})}{k} - \delta\right\} \leqslant e^{-\frac{\delta^2 k}{32}}$$

How to choose $\overline{A}$?

- Choose $\overline{A}_\ell = \textsc{maj}\{A^{\vec{j}}_\ell : \ell \in \vec{j}\}$
  does not work, have to use $\vec{i}$
- Choose $\overline{A}_\ell = \textsc{maj}\{A^{\vec{j}}_\ell : \ell \in \vec{j}, |\vec{j} \cap \vec{i}| \text{ large}, A^{\vec{j}} = A^{\vec{i}} \text{ on } \vec{i} \cap \vec{j}\}$
  maybe works, but tough to analyze

# General case

**Theorem**

*For any strategy* $\{A^{\vec{i}}\}_{\vec{i}}$*, there exists an* $\overline{A} = \overline{A}(B, \vec{i}, X_{\vec{i}})$ *such that*

$$\mathbf{P}\left\{ \frac{\mathsf{G}_n(\overline{A})}{n} \leqslant \frac{\mathsf{G}_k(A^{\vec{i}})}{k} - \delta \right\} \leqslant e^{-\frac{\delta^2 k}{32}}$$

How to choose $\overline{A}$?

- Choose $\overline{A}_\ell = \text{MAJ}\{A_\ell^{\vec{j}} : \ell \in \vec{j}\}$
  does not work, have to use $\vec{i}$
- Choose $\overline{A}_\ell = \text{MAJ}\{A_\ell^{\vec{j}} : \ell \in \vec{j}, |\vec{j} \cap \vec{i}| \text{ large}, A^{\vec{j}} = A^{\vec{i}} \text{ on } \vec{i} \cap \vec{j}\}$
  maybe works, but tough to analyze
- Optimal strategy?

# General case

**Theorem**

*For any strategy* $\{A^{\vec{i}}\}_{\vec{i}}$, *there exists an* $\overline{A} = \overline{A}(B, \vec{i}, X_{\vec{i}})$ *such that*

$$\mathbf{P}\left\{\frac{\mathsf{G}_n(\overline{A})}{n} \leqslant \frac{\mathsf{G}_k(A^{\vec{i}})}{k} - \delta\right\} \leqslant e^{-\frac{\delta^2 k}{32}}$$

How to choose $\overline{A}$?

- Choose $\overline{A}_\ell = \textsc{maj}\{A^{\vec{j}}_\ell : \ell \in \vec{j}\}$
  does not work, have to use $\vec{i}$
- Choose $\overline{A}_\ell = \textsc{maj}\{A^{\vec{j}}_\ell : \ell \in \vec{j}, |\vec{j} \cap \vec{i}|$ large, $A^{\vec{j}} = A^{\vec{i}}$ on $\vec{i} \cap \vec{j}\}$
  maybe works, but tough to analyze
- Optimal strategy? In what sense?

# Proof: introducing sequential exams

Notation: $\vec{i}^{p-1} = \vec{i}_1, \ldots, \vec{i}_{p-1}$

Two steps:

1. Introduce "sequential exams" and prove statement
2. Relate general strategies for a strategy for sequential exam

# Proof: introducing sequential exams

Notation: $\vec{i}^{p-1} = \vec{i}_1, \ldots, \vec{i}_{p-1}$

Two steps:

1. Introduce "sequential exams" and prove statement
2. Relate general strategies for a strategy for sequential exam

**Sequential exam** (or oral exam)

Interaction between examiner and student

- Questions one by one
- Have to answer $\vec{i}_p$ before getting $\vec{i}_{p+1}$
- After answering $\vec{i}_p$ also gets $X_{\vec{i}_p}$

# Proof: introducing sequential exams

Notation: $\vec{i}^{p-1} = \vec{i}_1, \ldots, \vec{i}_{p-1}$

Two steps:

1. Introduce "sequential exams" and prove statement
2. Relate general strategies for a strategy for sequential exam

**Sequential exam** (or oral exam)

Interaction between examiner and student

- Questions one by one
- Have to answer $\vec{i}_p$ before getting $\vec{i}_{p+1}$
- After answering $\vec{i}_p$ also gets $X_{\vec{i}_p}$

$\rightarrow A_p^{\text{seq}} = A_p^{\text{seq}}(\vec{i}_p, \vec{i}^{p-1}, X_{\vec{i}^{p-1}})$ but independent of $\vec{i}_{p+1} \ldots \vec{i}_k$

# Proof: introducing sequential exams

Notation: $\vec{i}^{p-1} = \vec{i}_1, \ldots, \vec{i}_{p-1}$

Two steps:

1. Introduce “sequential exams” and prove statement
2. Relate general strategies for a strategy for sequential exam

**Sequential exam** (or oral exam)

Interaction between examiner and student

- Questions one by one
- Have to answer $\vec{i}_p$ before getting $\vec{i}_{p+1}$
- After answering $\vec{i}_p$ also gets $X_{\vec{i}_p}$

$\to A_p^{\text{seq}} = A_p^{\text{seq}}(\vec{i}_p, \vec{i}^{p-1}, X_{\vec{i}^{p-1}})$ but independent of $\vec{i}_{p+1} \ldots \vec{i}_k$

Remark: A priori “general” and “sequential” incomparable

# Proof for sequential strategies

**Theorem**

*For any sequential strategy $A^{\text{seq}}$, there exists an $\overline{A} = \overline{A}(B, \vec{i}, X_{\vec{i}})$ such that*

$$\mathbf{P}\left\{ \frac{\mathsf{G}_n(\overline{A})}{n} \leqslant \frac{\mathsf{G}_k(A^{\vec{i}})}{k} - \delta \right\} \leqslant e^{-\frac{\delta^2 k}{8}}$$

Simplification: define $\overline{A}$ only on $\vec{j}$ with $|\vec{j}| = k$

$\rightarrow$ look at $\left[ \frac{\mathsf{G}_k(\overline{A})}{k} \leqslant \frac{\mathsf{G}_k(A^{\text{seq}})}{k} - \delta \right]$

# Proof for sequential strategies

**Theorem**

*For any sequential strategy $A^{\text{seq}}$, there exists an $\overline{A} = \overline{A}(B, \vec{i}, X_{\vec{i}})$ such that*

$$\mathbf{P}\left\{ \frac{\mathsf{G}_n(\overline{A})}{n} \leqslant \frac{\mathsf{G}_k(A^{\vec{i}})}{k} - \delta \right\} \leqslant e^{-\frac{\delta^2 k}{8}}$$

Simplification: define $\overline{A}$ only on $\vec{j}$ with $|\vec{j}| = k$
$\rightarrow$ look at $\left[\frac{\mathsf{G}_k(\overline{A})}{k} \leqslant \frac{\mathsf{G}_k(A^{\text{seq}})}{k} - \delta\right]$

$$\overline{A}_{\vec{j}_p} \stackrel{\text{def}}{=} A_p^{\text{seq}}(\vec{j}_p, \vec{i}^{p-1}, X_{\vec{i}^{p-1}})$$

*To answer all questions:* Partition $[n] = S_1 \cup \cdots \cup S_k$ at random, and for $\ell \in S_p$, let $\overline{A}_\ell = A^{\text{seq}}(\ell, \vec{i}^{p-1}, X_{\vec{i}^{p-1}})$

# Proof for sequential strategies

**Notation:** $\vec{i}^{p-1} = \vec{i}_1, \ldots, \vec{i}_{p-1}$   Grade $\mathsf{G}_k(A^{\text{seq}}) = \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{i}_p} = A_p^{\text{seq}}}$   Grade $\mathsf{G}_k(\overline{A}) = \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{j}_p} = \overline{A}_p}$

Using Azuma's inequality:

$$\mathbf{P}\left\{ \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{i}_p} = A_p^{\text{seq}}} - \sum_{p=1}^{k} \mathbf{E}_{\vec{i}_p, X_{\vec{i}_p}} \left\{ \mathbf{1}_{X_{\vec{i}_p} = A_p^{\text{seq}}} \middle| \vec{i}^{p-1} \vec{j}^{p-1} X_{\vec{i}^{p-1}} X_{\vec{j}^{p-1}} \right\} \geqslant \delta k \right\} \leqslant e^{-\frac{\delta^2 k}{2}}$$

$$\mathbf{P}\left\{ \sum_{p=1}^{k} \mathbf{E}_{\vec{j}_p, X_{\vec{j}_p}} \left\{ \mathbf{1}_{X_{\vec{j}_p} = \overline{A}_p} \middle| \vec{i}^{p-1} \vec{j}^{p-1} X_{\vec{i}^{p-1}} X_{\vec{j}^{p-1}} \right\} - \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{j}_p} = \overline{A}_p} \geqslant \delta k \right\} \leqslant e^{-\frac{\delta^2 k}{2}}$$

Observe:

$$\mathbf{E}\left\{ \mathbf{1}_{X_{\vec{i}_p} = A_p^{\text{seq}}} \middle| \vec{i}^{p-1} \vec{j}^{p-1} X_{\vec{i}^{p-1}} X_{\vec{j}^{p-1}} \right\} = \mathbf{E}\left\{ \mathbf{1}_{X_{\vec{j}_p} = \overline{A}_p} \middle| \vec{i}^{p-1} \vec{j}^{p-1} X_{\vec{i}^{p-1}} X_{\vec{j}^{p-1}} \right\}$$

$$\Rightarrow \qquad \mathbf{P}\left\{ \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{i}_p} = A_p^{\text{seq}}} - \sum_{p=1}^{k} \mathbf{1}_{X_{\vec{j}_p} = \overline{A}_p} \geqslant 2\delta k \right\} \leqslant 2e^{-\frac{\delta^2 k}{2}}$$

# Relating general to sequential strategies

**Theorem**

*There exists $A^{\text{seq}}$ such that for any $\{A^{\vec{i}}\}_{\vec{i}}$*

$$\mathbf{P}\left\{\sum_{p=1}^{k}\mathbf{1}_{X_{\vec{i}_p}=A^{\vec{i}}_p}-\sum_{p=1}^{k}\mathbf{1}_{X_{\vec{i}_p}=A^{\text{seq}}_p}\geqslant\delta k\right\}\leqslant e^{-\frac{\delta^2 k}{8}}$$

$$A^{\text{seq}}(\ell,\vec{i}^{p-1},X_{\vec{i}^{p-1}})\stackrel{\text{def}}{=}\text{ best guess for } X_\ell \text{ given } B,\vec{i}^{p-1},X_{\vec{i}^{p-1}}$$

$$\text{Azuma}\quad\Rightarrow\quad\sum_{p=1}^{k}\mathbf{1}_{X_{\vec{i}_p}=A^{\vec{i}}_p}\approx\sum_{p=1}^{k}\mathbf{E}_{\vec{i}_p,X_{\vec{i}_p}}\left\{\mathbf{1}_{X_{\vec{i}_p}=A^{\vec{i}}_p}\middle|\vec{i}^{p-1}X_{\vec{i}^{p-1}}(A^{\vec{i}})^{p-1}\right\}$$

$$\text{Azuma}\quad\Rightarrow\quad\sum_{p=1}^{k}\mathbf{1}_{X_{\vec{i}_p}=A^{\text{seq}}_p}\approx\sum_{p=1}^{k}\mathbf{E}_{\vec{i}_p,X_{\vec{i}_p}}\left\{\mathbf{1}_{X_{\vec{i}_p}=A^{\text{seq}}_p}\middle|\vec{i}^{p-1}X_{\vec{i}^{p-1}}(A^{\vec{i}})^{p-1}\right\}$$

For any fixed $\vec{i}_p$ and $B$, $(A^{\vec{i}})^{p-1}$ cannot help in predicting $X_{\vec{i}_p}$

$$\Longrightarrow\mathbf{E}_{\vec{i}_p,X_{\vec{i}_p}}\left\{\mathbf{1}_{X_{\vec{i}_p}=A^{\text{seq}}_p}\middle|\vec{i}^{p-1}X_{\vec{i}^{p-1}}(A^{\vec{i}})^{p-1}\right\}\geqslant\mathbf{E}_{\vec{i}_p,X_{\vec{i}_p}}\left\{\mathbf{1}_{X_{\vec{i}_p}=A^{\vec{i}}_p}\middle|\vec{i}^{p-1}X_{\vec{i}^{p-1}}(A^{\vec{i}})^{p-1}\right\}$$

# Recap of the proof

Start with $\{A^{\vec{i}}\}_{\vec{i}}$

$A^{\text{seq}}$ (guesses optimally given past) is at least as good on exam $\vec{i}$

If $A^{\text{seq}}$ works on $\vec{i}$, also works on rest

**Theorem**

*For any strategy $\{A^{\vec{i}}\}_{\vec{i}}$, there exists an $\overline{A} = \overline{A}(B, \vec{i}, X_{\vec{i}})$ such that*

$$\mathbf{P}\left\{ \frac{\mathsf{G}_n(\overline{A})}{n} \leqslant \frac{\mathsf{G}_k(A^{\vec{i}})}{k} - \delta \right\} \leqslant e^{-\frac{\delta^2 k}{32}}$$

# Quantum student $B$

System $B$ is quantum

Important difficulty: Applying $A^{\vec{i}}(B,\vec{i})$ affects $B$
Issues in the two steps of the classical proof

1. For sequential strategies, measurement may lead to losses
2. Cannot simultaneously define the two strategies

# Quantum student $B$

System $B$ is quantum

Important difficulty: Applying $A^{\vec{i}}(B, \vec{i})$ affects $B$
Issues in the two steps of the classical proof

1. For sequential strategies, measurement may lead to losses
2. Cannot simultaneously define the two strategies

In fact, as is, just wrong $\rightarrow$ QRAC example

# Quantum student $B$

System $B$ is quantum

Important difficulty: Applying $A^{\vec{i}}(B, \vec{i})$ affects $B$
Issues in the two steps of the classical proof

1. For sequential strategies, measurement may lead to losses
2. Cannot simultaneously define the two strategies

In fact, as is, just wrong $\rightarrow$ QRAC example

**Better way of quantifying correlation:**

- Use $H_{\max}(X_1 \dots X_n|B)$ (number of bits of hint for perfect recovery of $X_1 \dots X_n$)