Parallel Repetition of Interactive Arguments

Handout Mode

Iftach Haitner

Tel Aviv University.

December 15, 2011
Part I

Interactive Proofs and Arguments
\( \mathcal{NP} \) as a Non-interactive Proofs

**Definition 1 \((\mathcal{NP})\)**

\( \mathcal{L} \in \mathcal{NP} \) iff \( \exists \) and poly-time algorithm \( V \) such that:

1. \( \forall x \in \mathcal{L} \) there exists \( w \in \{0, 1\}^* \) s.t. \( V(x, w) = 1 \)
2. \( V(x, w) = 0 \) for every \( x \not\in \mathcal{L} \) and \( w \in \{0, 1\}^* \)

Only \( |x| \) counts for the running time of \( V \).

This proof system has

- Efficient verifier, efficient prover (given the witness)
- Soundness holds **unconditionally**
Interactive proofs/arguments

Protocols between efficient verifier and unbounded/efficient prover.

Definition 2 (Interactive proof)
A protocol \((P, V)\) is an interactive proof for \(L\), if \(V\) is a \(PPT\) and:

Completeness  \(\forall x \in L: \Pr[(P, V)(x) = 1] \geq 2/3\).

Soundness  \(\forall x \notin L, \text{ and any algorithm } P^*: \Pr[(P^*, V)(x) = 1] \leq 1/3\).

\(IP\) is the class of languages that have interactive proofs.

- \(IP = \text{PSPACE}\)!
- The above protocol has completeness error \(\frac{1}{3}\), and soundness error \(\frac{1}{3}\).
- We typically consider achieve (directly) perfect completeness.
- Smaller “soundness error" achieved via repetition.
- Relaxation: interactive arguments [also known as, Computationally sound proofs]: soundness only guaranteed against efficient \((PPT)\) provers.
- Games — no-input protocols.
Section 1

Interactive Proof for Graph Non-Isomorphism
Graph isomorphism

\( \Pi_m \) – the set of all permutations from \([m]\) to \([m]\)

**Definition 3 (graph isomorphism)**

Graphs \( G_0 = ([m], E_0) \) and \( G_1 = ([m], E_1) \) are isomorphic, denoted \( G_0 \equiv G_1 \), if there exists \( \pi \in \Pi_m \) such that
\[
(u, v) \in E_0 \text{ iff } (\pi(u), \pi(v)) \in E_1.
\]

\( \mathcal{GI} = \{(G_0, G_1) : G_0 \equiv G_1 \} \in \mathcal{NP} \)

Does \( \mathcal{GNI} = \{(G_0, G_1) : G_0 \not\equiv G_1 \} \in \mathcal{NP} \)?

We will show a simple interactive proof for \( \mathcal{GNI} \)

Idea: Beer tasting...
Interactive proof for \( GNI \)

**Protocol 4** \(((P, V)(G_0 = ([m], E_0), G_1 = ([m], E_1)))\)

1. \( V \) chooses \( b \leftarrow \{0, 1\} \) and \( \pi \leftarrow \Pi_m \), and sends \( \pi(E_b) \) to \( P \).
2. \( P \) send \( b' \) to \( V \) (tries to set \( b' = b \)).
3. \( V \) accepts iff \( b' = b \).

**Claim 5**

The above protocol is IP for \( GNI \), with perfect completeness and soundness error \( \frac{1}{2} \).
Proving Claim 5

- Graph isomorphism is an equivalence relation (separates all graph pairs into separate subsets)
- \([(m, \pi(E_i))]\) is a random element in \([G_i]\) — the equivalence class of \(G_i\)

Hence,

\[G_0 \equiv G_1: \Pr[b' = b] \leq \frac{1}{2}.
\]
\[G_0 \not\equiv G_1: \Pr[b' = b] = 1 \text{ (i.e., } P \text{ can, possibly inefficiently, extracted from } \pi(E_i))\]
Part II

Hardness Amplification
Hardness amplification

- In most settings we need **very small** soundness error (i.e., close to 0)
- Typically done by “amplifying the security” of an interactive proof/argument of **large** soundness error.
- Two main approaches:
  - **Sequential** repetition: achieves optimal amplification rate in almost any computation model, but increases the round complexity
  - **Parallel** repetition: sometimes does not achieve optimal amplification rate and sometimes achieves **nothing**

- How come parallel repetition might not work? **Example**
- Parallel repetition **does** achieve optimal amplification rate for interactive proofs and public-coin interactive arguments
- Public-coin interactive proof/argument — in each round the verifier flips coins and sends them to the prover. To compute its output, the verifier applies some (fixed) function to the protocol’s transcript.
Hardness amplification, cont.

- Give a protocol $\pi = (P, V)$ and $k \in \mathbb{N}$, let $\pi^{(k)} = (P^{(k)}, V^{(k)})$ be the $k$-fold parallel repetition of $\pi$: i.e., $k$ parallel independent copies of $\pi$

- Assume $\Pr[(\tilde{P}, V) = 1] \leq \varepsilon$ for any $s$-size algorithm $\tilde{P}$, we would like to prove that $\Pr[(\tilde{P}^{(k)}, V^{(k)}) = 1^k] \leq f(k)(\varepsilon)$ for any $s^{(k)}$-size algorithm $\tilde{P}^{(k)}$.

- Typically, $s^{(k)} = s \cdot \text{poly}(f(k)(\varepsilon)/k)$

- If $f(\varepsilon) = \varepsilon^{\Omega(k)}$, the above is an exponential-rate amplification (and hence optimal)

- If $f(\varepsilon) = \varepsilon^{\delta_1 \cdot k^{\delta_2}}$, the above is a weakly-exponential-rate amplification

- Why size?

- Concrete security

- In the following we focus on games (no input protocols)
Section 2

Parallel repetition of public-coin interactive argument
Parallel repetition of public-coin interactive argument

**Theorem 6**

Let $\pi = (P, V)$ be $m$-round, public-coin protocol with $\Pr[(\overline{P}, V) = 1] \leq \varepsilon$ for any $s$-size $\overline{P}$, then $\Pr[(\overline{P}^{(k)}, V^{(k)}) = 1^k] \leq \varepsilon^{k/4}$ for any $s \cdot \frac{\varepsilon^{k/4}}{mk^3s_V}$-size $\overline{P}^{(k)}$, where $s_V$ is $V$'s size.

Proof plan: Let $\overline{P}^{(k)}$ be $s^{(k)}$-size algorithm with $\Pr[(\overline{P}^{(k)}, V^{(k)}) = 1^k] = \varepsilon^{(k)}$, we construct $s^{(k)} \cdot \frac{mk^3s_V}{\varepsilon^{(k)}}$-size $\overline{P}$ with $\Pr[(\overline{P}, V) = 1] \geq (\varepsilon^{(k)})^{4/k}$.

- The $k/4$ in the exponent can be pushed to be almost $k$.
- Assume for simplicity that $\overline{P}^{(k)}$ is deterministic
- Assume w.l.o.g. that $V$ sends the first message in $\pi$ and that in each round it sends $\ell$ coins.
- We view the coins of $V^{(k)}$ as a matrix $R \in \{0, 1\}^{m \times (k\ell)}$, letting $R_j$ denote the coins of the $j$'th round
- Let $x^j = x_1, \ldots, x_j$ (hence $R^j$ denote the coins used in the first $j$ rounds).
- Let $R \sim \{0, 1\}^{m \times (k\ell)}$
Algorithm $\tilde{P}$

Let $q = k^2$.

Algorithm 7 ($\tilde{P}$)

1. Let $i^* \leftarrow [k]$.
2. Upon getting the $j$'th round message $r$ from $V$, do:
   
   2.1 Let $R \leftarrow \{0, 1\}^{m \times (k\ell)}$, conditioned that $R_1,...,j-1 = \tilde{R}_1,...,j-1$ and $R_{j,i^*} = r$.
   
   2.2 If $(P^{(k)}, V^{(k)}(R)) = 1^k$:
      
      2.2.1 Set $\tilde{R}_j = R_j$
      
      2.2.2 Send $a_{j,i^*}$ back to $V$, for $a_j$ being the $j$'th message $P^{(k)}$ send to $V^{(k)}$ in $(P^{(k)}, V^{(k)}(R))$.
      
      Else, GOTO Line 2.1
   
   2.3 Abort, if overall number of sampling exceeds $\lceil qm/\varepsilon^{(k)} \rceil$.

Let $\tilde{P}'$ be the non aborting variant of $\tilde{P}$, let $\tilde{R}$ and $\tilde{N}$ be the value of $\tilde{R}$ and # of samples done in a random execution of $(\tilde{P}', V^{(k)})$, respectively.

$\Pr[(\tilde{P}, V) = 1] \geq \Pr\left[\text{win}(\tilde{R}, \tilde{N}) := (P^{(k)}, V^{(k)}(\tilde{R})) = 1^k \land \tilde{N} \leq qm/\varepsilon^{(k)}\right]$. 
Ideal “attacker”

**Experiment 8 (\(\hat{P}\))**

For \(j = 1\) to \(m\):

1. Let \(R \leftarrow \{0, 1\}^{m \times (k \ell)}\), conditioned that \(R_{1,\ldots,j-1} = \hat{R}_{1,\ldots,j-1}\).

2. If \((\tilde{P}(k), V(k)(R)) = 1^k\), set \(\hat{R}_j = R_j\). Else, GOTO Line 1.

\(\Rightarrow\) Let \(\hat{R}\) be the value of \(\hat{R}\) in the end of a random execution of \(\hat{P}\).

\(\Rightarrow\) \(\hat{R} \sim R|_{(\tilde{P}(k), V(k)(R)) = 1^k}\)

\(\Rightarrow\) In particular, \(\Pr[(\tilde{P}(k), V(k)(\hat{R}) = 1^k)] = 1\)

\(\Rightarrow\) Let \(\hat{N}\) be \# of samples done in \(\hat{P}\).

**Lemma 9**

\[\Pr[\hat{N} > qm/\varepsilon(k)] < \frac{1}{q}\]

Hence, \(\Pr[\text{win}(\hat{R}, \hat{N})] = \Pr[(\tilde{P}(k), V(k)(\hat{R})) = 1^k \land \hat{N} \leq qm/\varepsilon(k)] \geq 1 - \frac{1}{q}\)
Proving Lemma 9 — Pr \[ \hat{N} > qm/\varepsilon^{(k)} \] < \frac{1}{q}

\begin{itemize}
\item Let \((X_1, \ldots, X_m) = R\) and \((Y_1, \ldots, Y_m) = \hat{R}\)

\item For \(y \in \text{Supp}(Y_j)\), let
\[ v(y) := \text{Pr} \left[ (P^{(k)}, V^{(k)}(X^m) = 1^k | X^j = y) \right] \]

\item Conditioned on \(Y_j = y\), the expected \# of samples done in \((j + 1)\)’th round of \(\hat{P}\) is \(\frac{1}{v(y)}\).

\item We prove Lemma 9 showing that \(E \left[ \frac{1}{v(Y_j)} \right] \leq \frac{1}{\varepsilon^{(k)}}\) for every \(j \in \{0, \ldots, m - 1\}\)
\end{itemize}

Claim 10

For \(j \in \{0, \ldots, m - 1\}\) and \(y \in \text{Supp}(Y_j)\), it holds that \(\text{Pr}_{Y_j}[y] = \text{Pr}_{X_j}[y] \cdot \frac{v(y)}{\varepsilon^{(k)}}\)

Hence, \(E \left[ \frac{1}{v(Y_j)} \right] = \sum_{y \in \text{Supp}(Y_j)} \text{Pr}[Y_j = y] \cdot \frac{1}{v(y)} = \sum_{y \in \text{Supp}(Y_j)} \text{Pr}[X_j = y] \cdot \frac{v(y)}{\varepsilon^{(k)}} \cdot \frac{1}{v(y)} = \frac{1}{\varepsilon^{(k)}} \cdot \sum_{y \in \text{Supp}(Y_j)} \text{Pr}[X_j = y] \leq \frac{1}{\varepsilon^{(k)}}\). \(\square\)
Proving Claim 10 — $\Pr_{Y_j}[y] = \Pr_{X_j}[y] \cdot \frac{v(y)}{\varepsilon(k)}$

Recall $v(y) := \Pr[(\overline{P(k)}, V(k)(X^m) = 1^k | X^j = y)]$. Note that

$$\begin{align*}
\Pr_{Y_j|Y_{j-1}=y_1\ldots j-1}[y_j] &= \sum_{\ell=1}^{\infty} (1 - v(y_1\ldots j-1))^{\ell-1} \cdot \Pr_{X_j|X_{j-1}=y_1\ldots j-1}[y_j] \cdot v(y) \\
&= \frac{1}{v(y_1\ldots j-1)} \cdot \Pr_{X_j|X_{j-1}=y_1\ldots j-1}[y_j] \cdot v(y)
\end{align*}$$

(Eq. 1)

The proof proceeds by induction on $j$.

$$\begin{align*}
\Pr_{Y_j}[y] &= \Pr_{Y_{j-1}}[y_1\ldots j-1] \cdot \Pr_{Y_j|Y_{j-1}=y_1\ldots j-1}[y_j] \\
&= \Pr_{X_{j-1}}[y_1\ldots j-1] \cdot \frac{v(y_1\ldots j-1)}{\varepsilon(k)} \cdot \Pr_{Y_j|Y_{j-1}=y_1\ldots j-1}[y_j] \quad \text{(i.h.)}
\end{align*}$$

$$\begin{align*}
&= \Pr_{X_{j-1}}[y_1\ldots j-1] \cdot \frac{v(y_1\ldots j-1)}{\varepsilon(k)} \cdot \frac{v(y)}{v(y_1\ldots j-1)} \cdot \Pr_{X_j|X_{j-1}=y_1\ldots j-1}[y_j] \\
&= \Pr_{X_j}[y] \cdot \frac{v(y)}{\varepsilon(k)}.
\end{align*}$$
From ideal to real

Let \( \tilde{I} \) be the value of \( i^* \) in \( \tilde{P} \).

**Claim 11**

\[
D(\hat{R}, \hat{N} || \tilde{R}, \tilde{N}) \leq \frac{1}{k} \sum_{i \in [k]} D(\hat{R} || \tilde{R}_{|\tilde{I} = i}).
\]

**Claim 12**

\[
\sum_{i \in [k]} D(\hat{R} || \tilde{R}_{|\tilde{I} = i}) \leq D(\hat{R} || R).
\]

1. Thm. 7 in Lecture 7 \( \implies \) \( D(\hat{R} || R) \leq \log \frac{1}{\Pr[(P^{(k)}, V^{(k)}(R)) = 1^k]} \leq \log \frac{1}{\varepsilon(k)} \)

2. Hence, \( D(\text{win}(\hat{R}, \hat{N}) || \text{win}(\tilde{R}, \tilde{N})) \leq D(\hat{R}, \hat{N} || \tilde{R}, \tilde{N}) \leq -\frac{1}{k} \cdot \log \varepsilon(k) \)

3. Lemma 15 \( \implies \) \( \alpha := \Pr[\text{win}(\hat{R}, \hat{N})] \geq 1 - \frac{1}{q} \), and let \( \beta := \Pr[\text{win}(\tilde{R}, \tilde{N})] \).

4. By (2), \( \alpha \cdot \log \frac{\alpha}{\beta} + (1 - \alpha) \log \frac{1-\alpha}{1-\beta} \leq -\frac{1}{k} \cdot \log \varepsilon(k) \)

   \( \implies \beta \geq 2^{\log \alpha + \frac{1-\alpha}{\alpha} \log(1-\alpha) + \frac{1}{\alpha k} \log \varepsilon(k)} \)

5. Since \( q = k^2 \): \( \alpha \geq 2^{-\frac{2}{q}} \geq 2^{-\frac{1}{k}} \) and \( \frac{1-\alpha}{\alpha} \log(1-\alpha) \geq -\frac{4 \log k}{k^2} \geq -\frac{1}{k} \)

6. We conclude that \( \beta \geq 2^{\frac{4 k}{k} \log \varepsilon(k)} = k^{4 / \sqrt{\varepsilon(k)}}. \square \)
Proving Claim 12 — \( \sum_{i \in [k]} D(\hat{R} \mid \tilde{R}_{\tilde{i} = i}) \leq D(\hat{R} \mid R) \)

**Lemma 13**

Let \( Z = \{Z_{ij}\}_{(i,j) \in [k] \times [m]} \) be iids and let \( W \) be an event. For \( z \in \text{Supp}(Z) \), let

\[
\xi_i(z) := \prod_{j=1}^{m} \Pr[Z_{j,i} = z_{i,j}] \cdot \Pr[Z_{j,-i} = z_{i,j-1} \mid Z_1, \ldots, j-1 = z_1, \ldots, j-1 \land Z_j,i = z_{i,j} \land W].
\]

Then \( \sum_{i=1}^{k} D(Z \mid w \mid \xi_i) \leq D(Z \mid w \mid Z) \).

Letting \( Z = R \) and \( W \) be the event \((\hat{P}^{(k)}, V^{(k)}(R)) = 1^k\), Lemma 13 yields that

\[
\sum_{i \in [k]} D(\hat{R} \mid \tilde{R}_{\tilde{i} = i}) = \sum_{i \in [k]} D(R \mid w \mid \tilde{R}_{\tilde{i} = i}) \leq D(R \mid w \mid R) = D(\hat{R} \mid R). \quad \Box
\]
Proving Lemma 13

We prove for \( m = k = 2 \).

\[ Z = (X_0, X_1, Y_0, Y_1) \text{ iids and } W \text{ an event.} \]

\[ \xi_i(x_0, x_1, y_0, y_1) := \Pr[X_i = x_i] \cdot \Pr[X_i = x_i \mid X_i = x_i \wedge W] \cdot \Pr[Y_i = y_i] \cdot \Pr[Y_i = y_i \mid Y_i = y_i \wedge (X_0, X_1) = (x_0, x_1) \wedge W]. \]

We need to prove that \( \sum_{i=1}^{2} D(Z \mid W \mid \xi_i) \leq D(Z \mid W \mid Z) \).

- Let \( U = p_Z \) and \( C = p_{Z \mid W} \).
- Let \( X = (X_0, X_1) \)

\[ Q(x_0, x_1, y_0, y_1) := \Pr[X_0 = x_0 \mid W] \cdot \Pr[X_1 = x_1 \mid W] \cdot \Pr[Y_0 = y_0 \mid W, X = (x_0, x_1)] \cdot \Pr[Y_1 = y_1 \mid W, X = (x_0, x_1)] \]

- We write \( \frac{C(x_0, x_1, y_0, y_1)}{Q(x_0, x_1, y_0, y_1)} = \frac{\Pr[X_0 = x_0 \mid W] \cdot \Pr[Y_0 = y_0 \mid W, X = (x_0, x_1)]}{\Pr[X_0 = x_0] \cdot \Pr[Y_0 = y_0]} \cdot \frac{\Pr[X_1 = x_1 \mid W] \cdot \Pr[Y_1 = y_1 \mid W, X = (x_0, x_1)]}{\Pr[X_1 = x_1] \cdot \Pr[Y_1 = y_1]} \cdot \frac{C(x_0, x_1, y_0, y_1)}{Q(x_0, x_1, y_0, y_1)} \)
Proving Lemma 13, cont.

\[ D(C||U) = \mathbb{E}_{(x_0, x_1, y_0, y_1) \leftarrow C} \left[ \log \frac{\Pr[X_0 = x_0|W] \cdot \Pr[Y_0 = y_0|W, X = (x_0, x_1)]}{\Pr[X_0 = x_0] \cdot \Pr[Y_0 = y_0]} \right] + \mathbb{E}_{(x_0, x_1, y_0, y_1) \leftarrow C} \left[ \log \frac{\Pr[X_1 = x_1|W] \cdot \Pr[Y_1 = y_1|W, X = (x_0, x_1)]}{\Pr[X_1 = x_1] \cdot \Pr[Y_1 = y_1]} \right] + \mathbb{E}_{(x_0, x_1, y_0, y_1) \leftarrow C} \left[ \log \frac{C(x_0, x_1, y_0, y_1)}{Q(x_0, x_1, y_0, y_1)} \right]. \]

It follows that

\[ D(C||U) = D(X_0|w, X_1|w, x_0, Y_0|w, x, Y_1|w, x, y_0||X_0, X_1|w, x_0, Y_0, Y_1|w, x, y_0) + D(X_1|w, X_1|w, x_1, Y_1|w, x, y_1||X_1, X_1|w, x_1, Y_1, Y_1|w, x, y_1) + D(C||Q) \]

\[ = \sum_{i=1}^{2} D(Z|w||\xi_i) + D(C||Q) \]

\[ \geq \sum_{i=1}^{2} D(Z|w||\xi_i). \qed \]
Ideal “attacker”, variant

Experiment 14 (\(\hat{P}\))

1. Let \(i^* \leftarrow [k]\).

2. For \(j = 1\) to \(m\):

   2.1 Let \(R \leftarrow \{0, 1\}^{m \times (k\ell)}\), conditioned on \(R_1, \ldots, j-1 = \hat{R}_1, \ldots, j-1\).

   2.2 If \((\hat{P}(k), V(k)(R)) = 1^k\), set \(\hat{R}_{j,i^*} = R_{j,i^*}\). Else, GOTO Line 2.1.

   2.3 Let \(R \leftarrow \{0, 1\}^{m \times \ell}\), conditioned on \(R_1, \ldots, j-1 = \hat{R}_1, \ldots, j-1\) and \(R_{j,i^*} = \hat{R}_{j,i^*}\).

   2.4 If \((\hat{P}(k), V(k)(R)) = 1^k\), set \(\hat{R}_j = R_j\). Else, GOTO Line 2.3.

Let \(\hat{R}\) be the final value of \(\hat{R}\) in \(\hat{P}\).

Let \(\hat{N}\) be the \# of Step-2.3-samples done in \(\hat{P}\).

Lemma 15 (essentially the same proof as of Lemma 9)

\[
\Pr\left[\text{win}(\hat{R}, \hat{N})\right] = \Pr\left[(\hat{P}(k), V(k)(\hat{R})) = 1^k \wedge \hat{N} \leq qm/\varepsilon(k)\right] \geq 1 - \frac{1}{q}
\]
Proving Claim 11 — \( D(\hat{R}, \hat{N} \| \tilde{R}, \tilde{N}) \leq \frac{1}{k} \sum_{i \in [k]} D(\hat{R} \| \tilde{R}_{|i=i}) \)

Let \( \hat{I} \) be the value of \( i^* \) in \( \hat{P} \) (recall that \( \tilde{I} \) is the value of \( i^* \) in \( \tilde{P} \)).

Let \( (\tilde{R}(i), \tilde{N}(i)) = (\tilde{R}, \tilde{N})_{|i=i} \) and \( (\hat{R}(i), \hat{N}(i)) = (\hat{R}, \hat{N})_{|i=i} \). Note that \( \hat{R}(i) = \hat{R} \).

\[
D(\hat{R}, \hat{N} \| \tilde{R}, \tilde{N}) \leq D(\hat{R}, \hat{N}, \hat{I} \| \tilde{R}, \tilde{N}, \hat{I})
\]

(data-processing)

\[
= D(\hat{I} \| \hat{I}) + \frac{1}{k} \sum_{i \in [k]} D(\hat{R}(i), \hat{N}(i) \| \tilde{R}(i), \tilde{N}(i))
\]

(chain rule)

\[
= \frac{1}{k} \sum_{i \in [k]} D(\hat{R}_i, \hat{N}(i) \| \tilde{R}(i), \tilde{N}(i))
\]

For \( i \in [k] \), it holds that

\[
D(\hat{R}(i), \hat{N}(i) \| \tilde{R}(i), \tilde{N}(i)) = D(\hat{R}(i) \| \tilde{R}(i)) + \mathbb{E}_{r \leftarrow \tilde{R}(i)} \left[ D(\hat{N}(i) \| \tilde{R}(i) = r \| \tilde{N}(i) \| \tilde{R}(i) = r) \right]
\]

(chain rule)

\[
= D(\hat{R}(i) \| \tilde{R}(i)) \quad \text{(since } \hat{N}(i) \| \tilde{R}(i) = r \equiv \tilde{N}(i) \| \tilde{R}(i) = r) \]

Hence, \( D(\hat{R}, \hat{N} \| \tilde{R}, \tilde{N}) \leq \frac{1}{k} \sum_{i \in [k]} D(\hat{R}(i) \| \tilde{R}(i)) \) \( \square \)
Parallel repetition of interactive proofs

▶ Similar proof to the public-coin proof we gave above.

▶ In each round, the attacker $\tilde{P}$ samples random continuations of $(P^{(k)}, V^{(k)})$, till he gets an accepting execution.

▶ Why fails us to extend this approach for non-public-coin interactive arguments?
Section 3

Parallel amplification for any interactive argument
Parallel amplification theorem for any protocol

- Can we amplify the security of any interactive argument “in parallel”?
- Yes we can!
Relevant papers

  
The proof given in class is in the spirit of this paper.