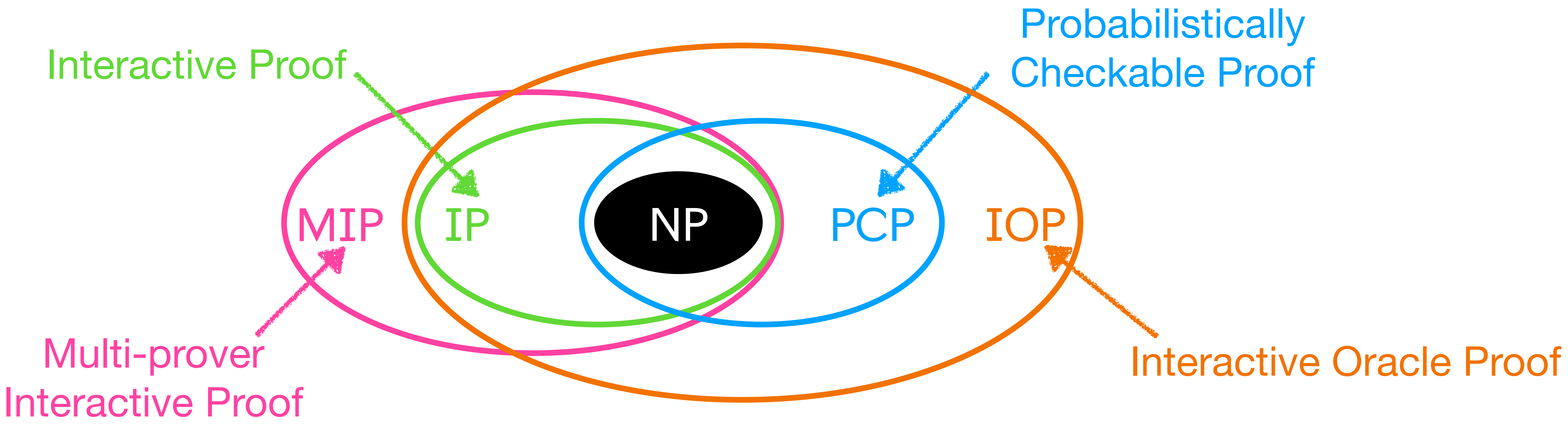
On Parallel Repetition of PCPs

Alessandro Chiesa, Ziyi Guan, Burcu Yıldız

What is parallel repetition?

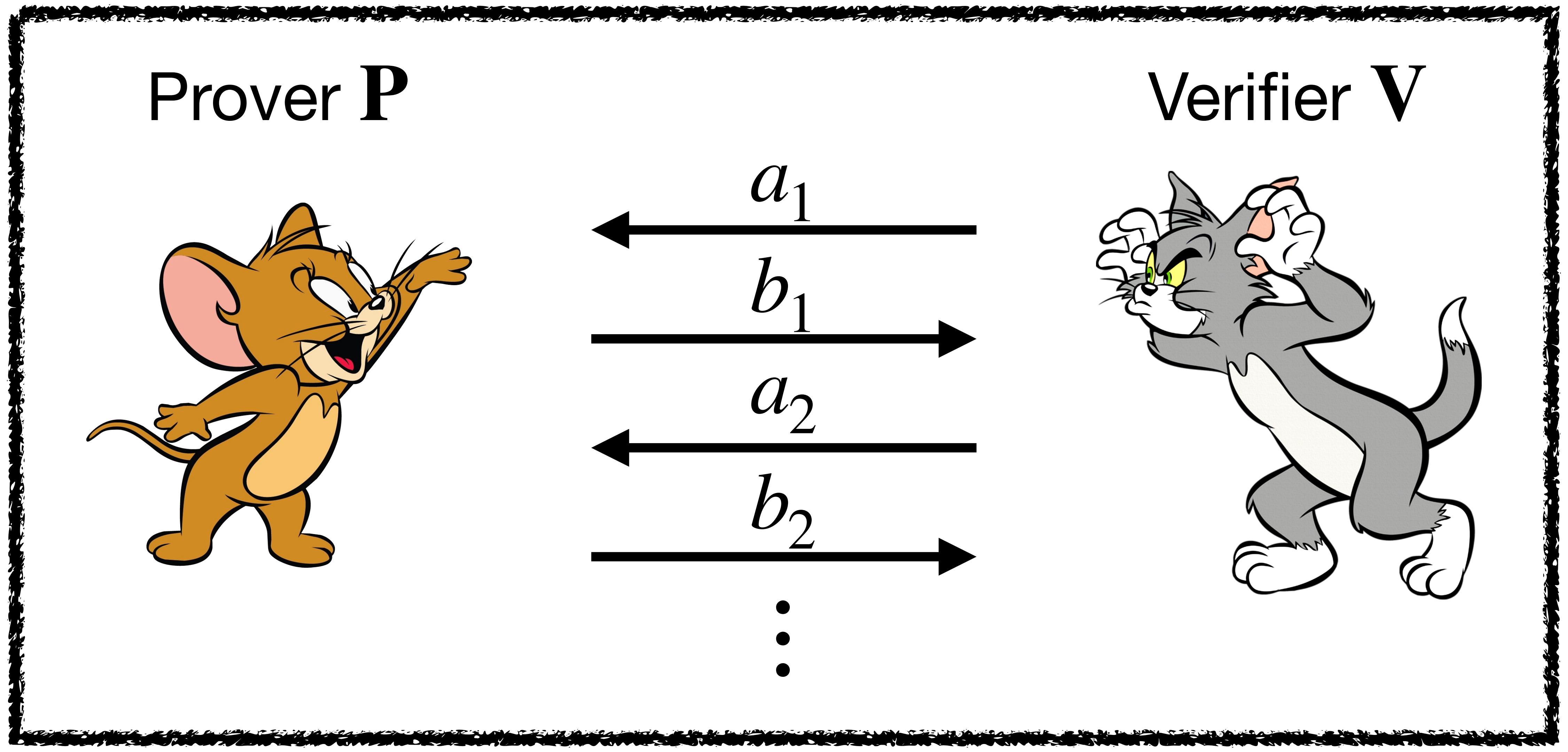
Probabilistic proof systems



Fundamental question: How to `reduce soundness error` for probabilistic proofs?

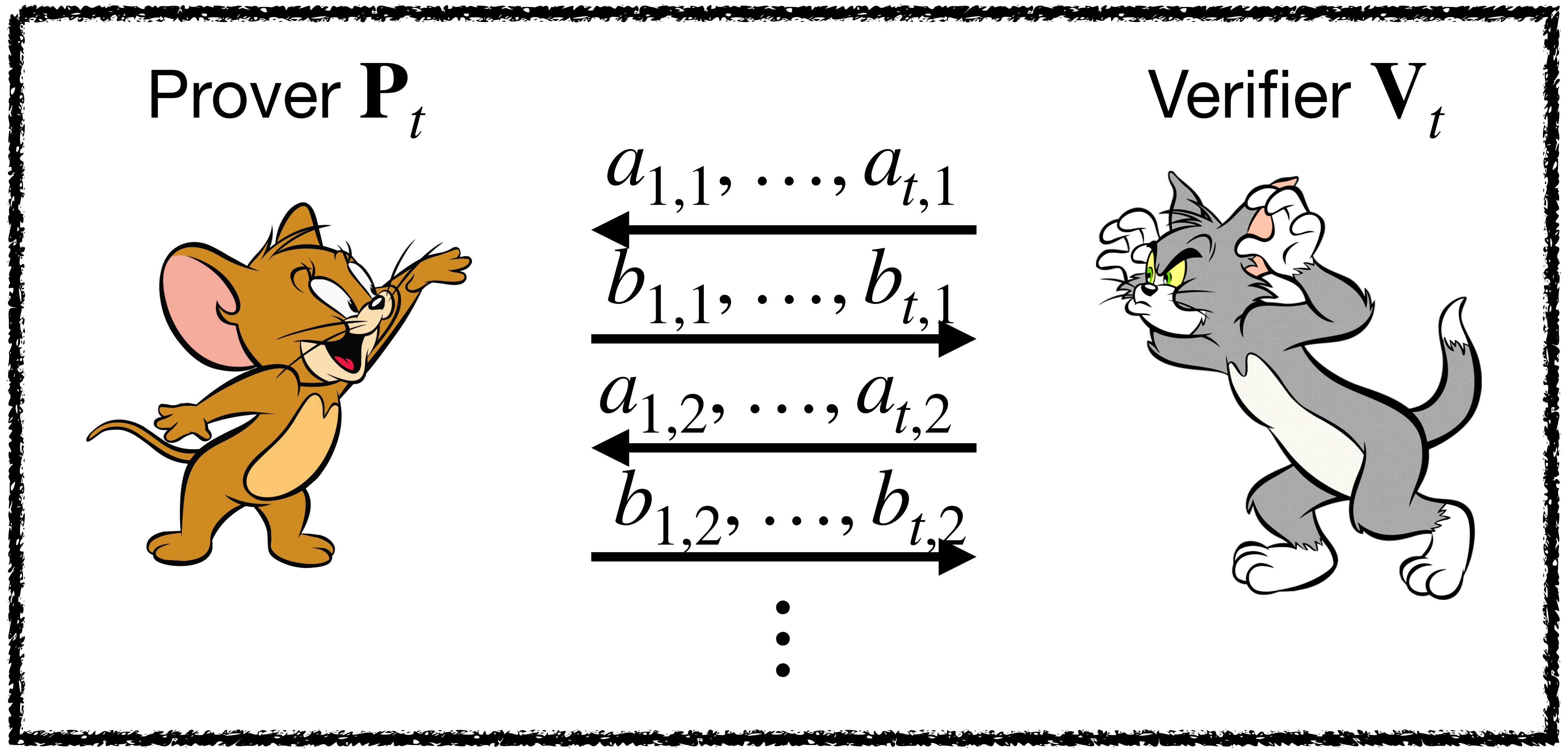
- Rerun the proof system for t times: soundness error $\beta \mapsto \beta^t$, but other efficiency measures increase as t increases.
  - Sometimes we call this rerunning strategy the sequential repetition.
- Parallel repetition: reduce soundness error while preserve key efficiency measures.
  - Defined differently for different probabilistic proofs.

Parallel repetition for IPs (interactive proofs)



Sequential repetition:
Round complexity k $\mapsto t \cdot$ k

t-wise parallel repetition



Round complexity k $\mapsto$ k ✅

Prover communication complexity $\mathrm{pc} \mapsto t \cdot \mathrm{pc}$

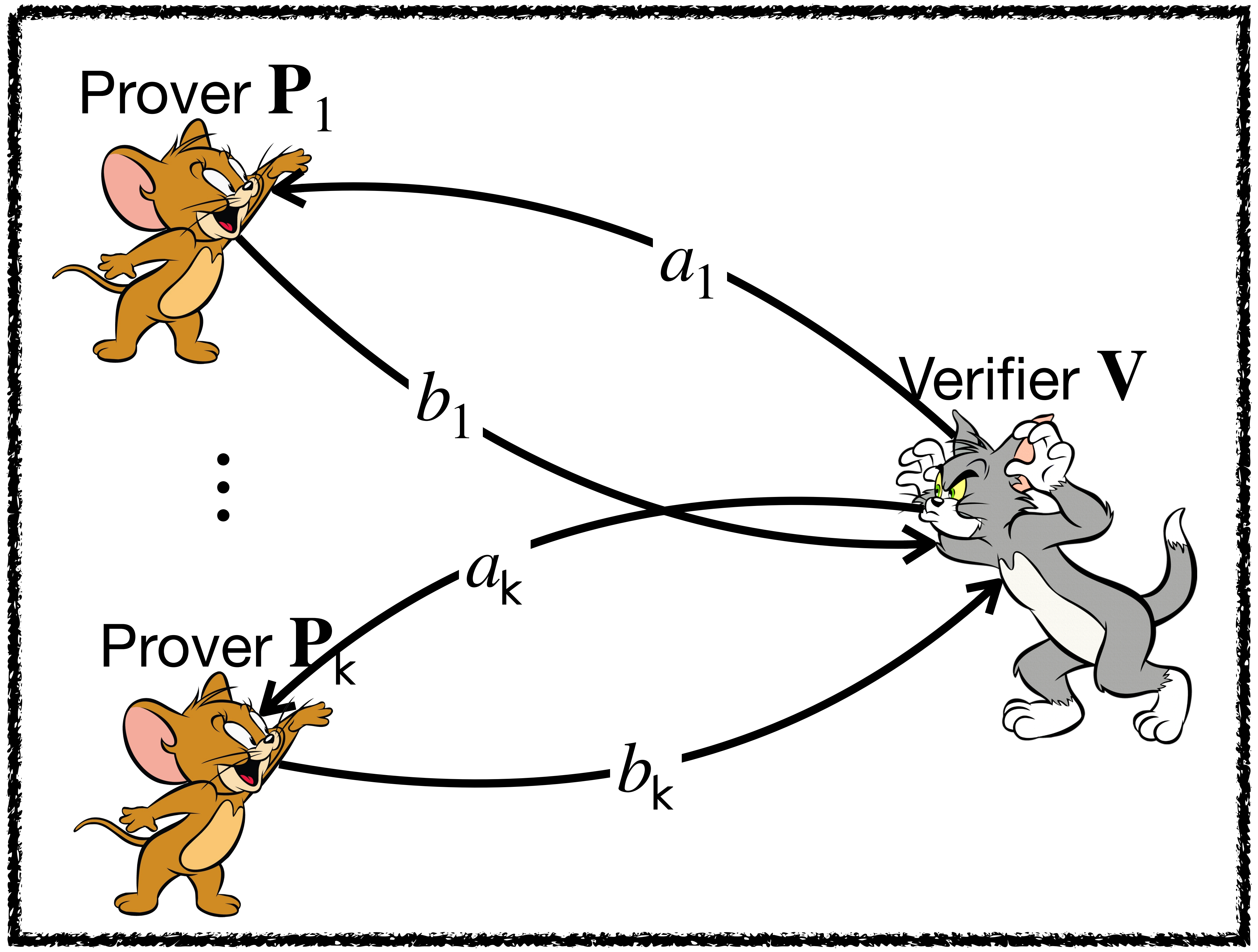
Verifier communication complexity $\mathrm{vc} \mapsto t \cdot \mathrm{vc}$

Verifier randomness complexity r $\mapsto t \cdot$ r

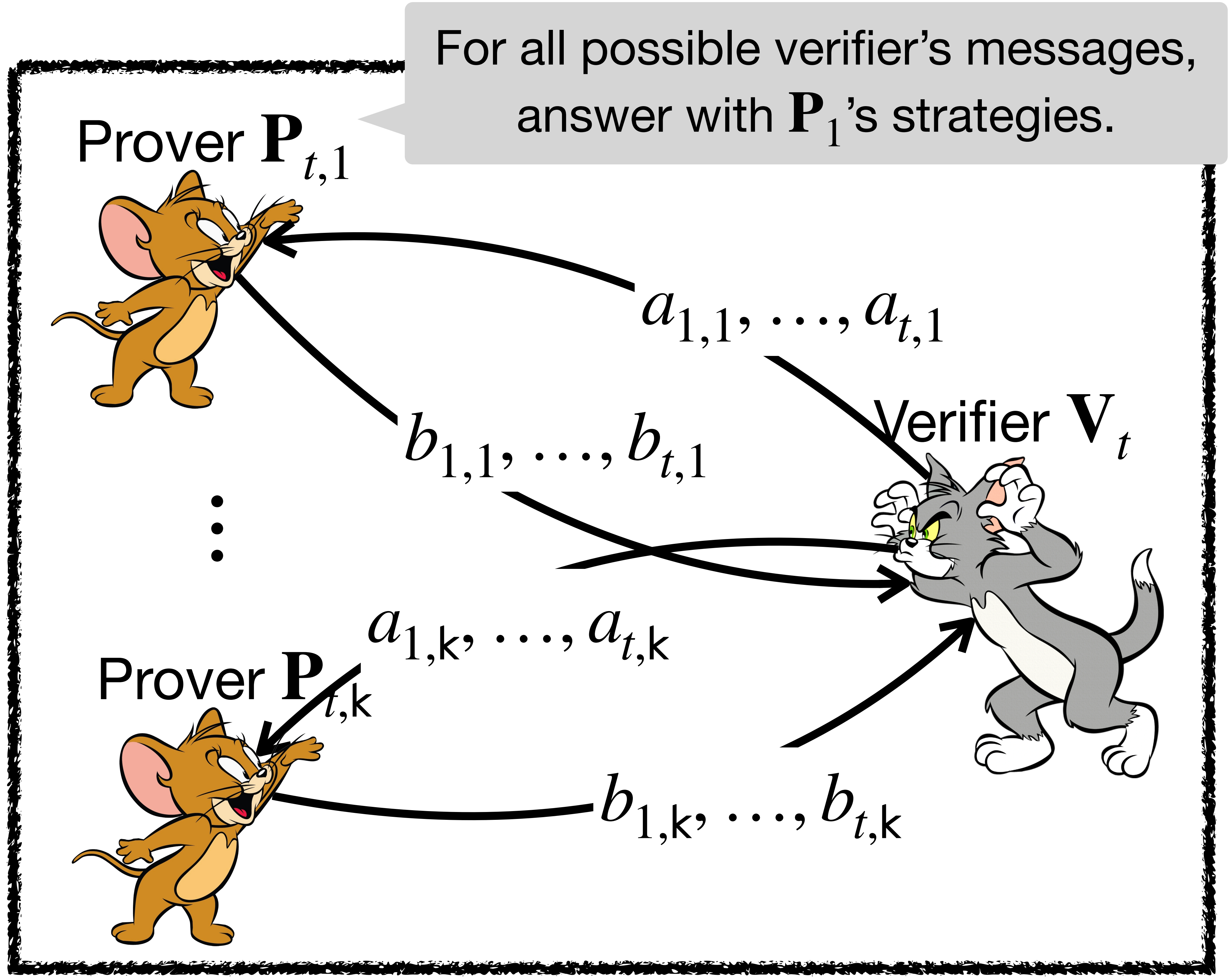
How about the soundness error?

- Soundness error $\beta \mapsto \beta^t$ ✅

Parallel repetition for MIPs (multi-prover interactive proofs)



t-wise parallel repetition



Number of provers k $\mapsto$ k ✅
Round complexity preserved ✅

Prover communication complexity $\mathrm{pc} \mapsto t \cdot \mathrm{pc}$

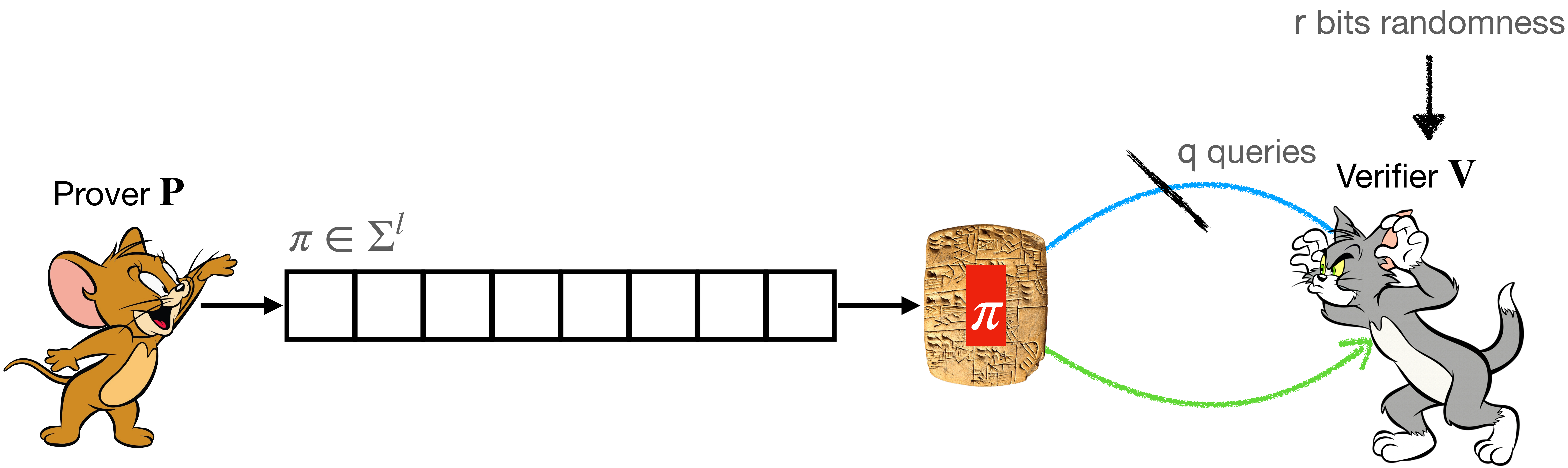
Verifier communication complexity $\mathrm{vc} \mapsto t \cdot \mathrm{vc}$

Verifier randomness complexity r $\mapsto t \cdot$ r

How about the soundness error?

- $\beta^t \le \beta_t \le \beta$
- Soundness error $\beta < 1 \implies \lim_{t \to \infty} \beta_t = 0$ [Verbitsky96]
- 2-prover MIP: $\beta_t \le \beta^{c_V \cdot t}$ [Raz98]
- k-prover MIP: open
- Not as good as parallel repetition for IP

Probabilistically checkable proof (PCP)

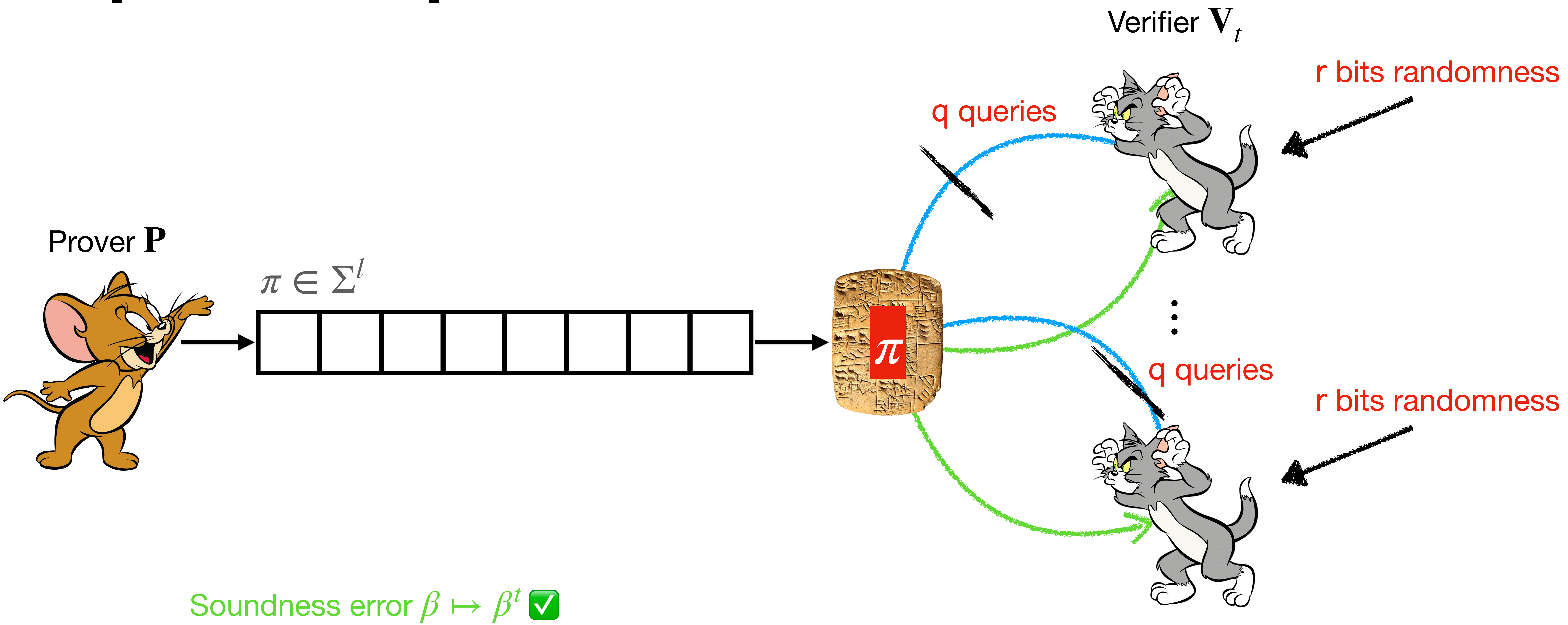


Perfect completeness: for every $x \in L$, let $\pi := \mathbf{P}(x)$, $\Pr_{\rho \leftarrow \{0,1\}^{\mathsf{r}}}\left[\mathbf{V}^{\pi}(x;\rho) = 1\right] = 1$.

Soundness: for every $x \notin L$ and $\tilde{\pi} \in \Sigma^l$, $\Pr_{\rho \leftarrow \{0,1\}^{\mathsf{r}}}\left[\mathbf{V}^{\tilde{\pi}}(x;\rho) = 1\right] \leq \beta$.

How to **reduce soundness error** for PCPs?

Sequential repetition for PCPs



Soundness error $\beta \mapsto \beta^t$ ✅

Query complexity q $\mapsto t \cdot$ q

Parallel repetition for PCPs [1/3]

$t \cdot \mathsf{r}$ bits randomness

Natural definition of parallel repetition: e.g. [DM11]

Prover $\mathbf{P}_t$

$$\Pi := ((\pi[q_1], \ldots, \pi[q_t]))_{(q_1,\ldots,q_t)\in[l]^t} \in \left(\Sigma^t\right)^{l^t}$$

For all possible verifier's queries, answer with π's strategies.

q queries

Verifier $\mathbf{V}_t$

	ρ_1	ρ_2	$\ldots$	ρ_t
$\mathbf{Q}_1$	$Q_1[1]$	$Q_2[1]$	$\ldots$	$Q_t[1]$
$\mathbf{Q}_2$	$Q_1[2]$	$Q_2[2]$	$\ldots$	$Q_t[2]$
$\vdots$		$\vdots$		
$\mathbf{Q}_\mathsf{q}$	$Q_1[\mathsf{q}]$	$Q_2[\mathsf{q}]$	$\ldots$	$Q_t[\mathsf{q}]$

1. Sample t randomness for $\mathbf{V}$: $(\rho_i)_{i\in[t]} \leftarrow \left(\{0,1\}^{\mathsf{r}}\right)^t$.
2. Compute query lists of $\mathbf{V}$: $Q_i := \mathbf{V}_q(x; \rho_i)$.
3. Compute queries of $\mathbf{V}_t$: $\mathbf{Q}_i := \left(Q_j[i]\right)_{j\in[t]}$.
4. Query the PCP string Π: $\mathbf{ans}_i := \Pi[\mathbf{Q}_i]$.
5. Check that for every repetition $i \in [t]$: $\mathbf{V}_d\left(x, \rho_i, \left(\mathbf{ans}_j[i]\right)_{j\in[\mathsf{q}]}\right)$.

Parallel repetition for PCPs [2/3]

E.g.: 2-wise parallel repetition of a 3-query PCP

- Verifier $\mathbf{V}_2$ samples ρ_1 and ρ_2 for the two repetitions.
- Assume $Q_1 = (q_{1,1}, q_{1,2}, q_{1,3})$ and $Q_2 = (q_{2,1}, q_{2,2}, q_{2,3})$.
- $\mathbf{Q}_1 := (q_{1,1}, q_{2,1})$, $\mathbf{Q}_2 := (q_{1,2}, q_{2,2})$ and $\mathbf{Q}_3 := (q_{1,3}, q_{2,3})$.

$\pi = (a, b, c, d, e)$

Second position in $\mathbf{V}_2$'s query

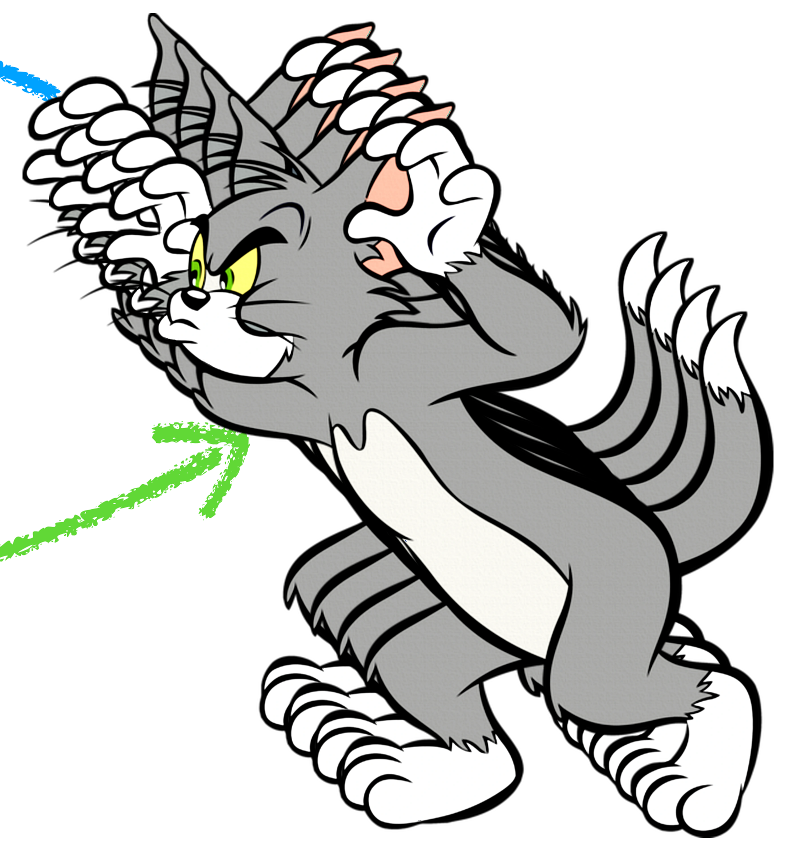
First position in $\mathbf{V}_2$'s query

Π	1	2	3	4	5
1	(a,a)	(a,b)	(a,c)	(a,d)	(a,e)
2	(b,a)	(b,b)	(b,c)	(b,d)	(b,e)
3	(c,a)	(c,b)	(c,c)	(c,d)	(c,e)
4	(d,a)	(d,b)	(d,c)	(d,d)	(d,e)
5	(e,a)	(e,b)	(e,c)	(e,d)	(e,e)

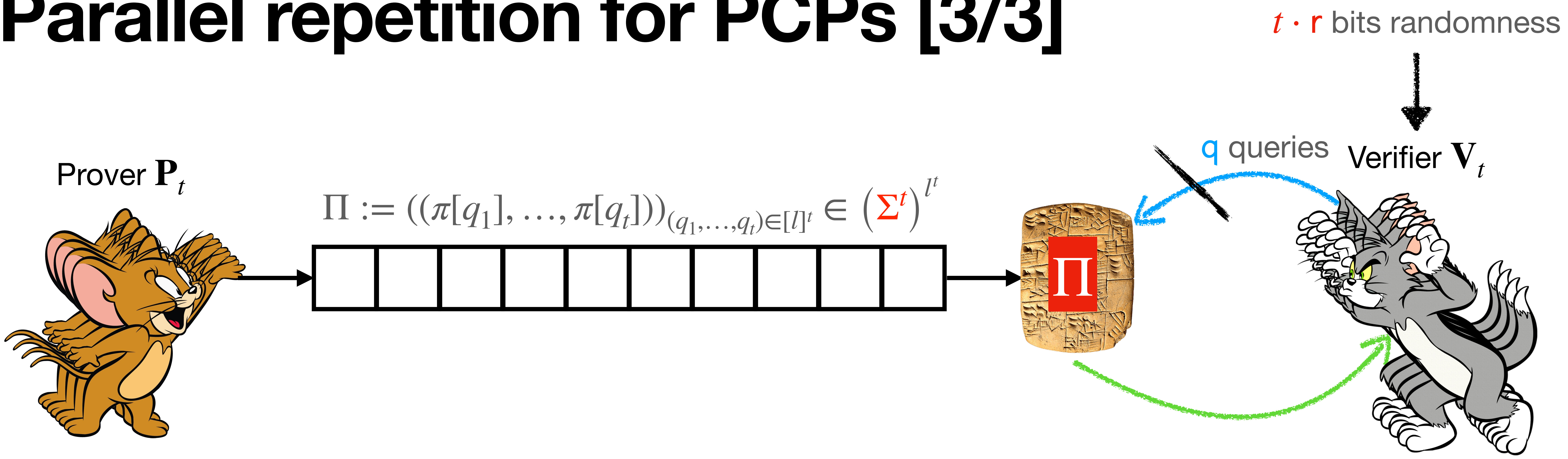
3 queries

Verifier $\mathbf{V}_2$

$2 \cdot$ r bits randomness



Parallel repetition for PCPs [3/3]



Query complexity q $\mapsto$ q ✅

Alphabet size $\Sigma \mapsto \Sigma^t$

Proof length $l \mapsto l^t$

Verifier randomness complexity r $\mapsto t \cdot$ r

What is the soundness error?

Our results

Result 1. Parallel repetition for PCP doesn't work: For a wide range of NP-complete languages, parallel repetition brings the limit of soundness error to 1.

Result 2. Parallel repetition for a PCP works if and only if the **MIP projection of the PCP** has non-trivial soundness.

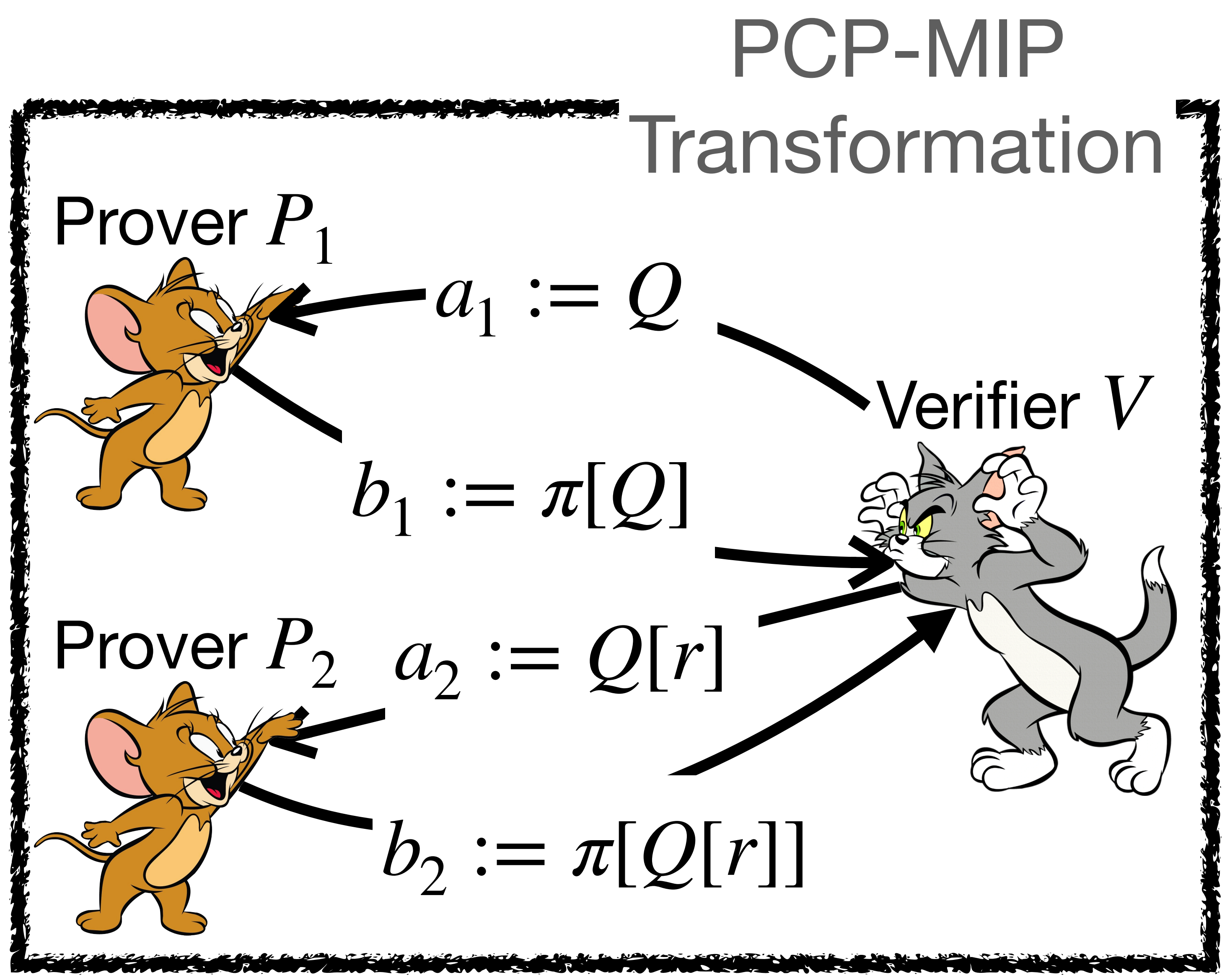
Result 3. Rate of decay of parallel repetition for some PCPs cannot be better than that for MIPs.

Result 4. Consistent parallel repetition (a variant of parallel repetition that we defined) for PCPs work as expected with exponential rate of decay.

Isn't parallel repetition for PCP used previously?

e.g. Hardness of approximation

Too expensive! Soundness error $\beta \mapsto 1 - \frac{1-\beta}{q}$



Step 1. Transform a PCP to a 2-prover MIP.

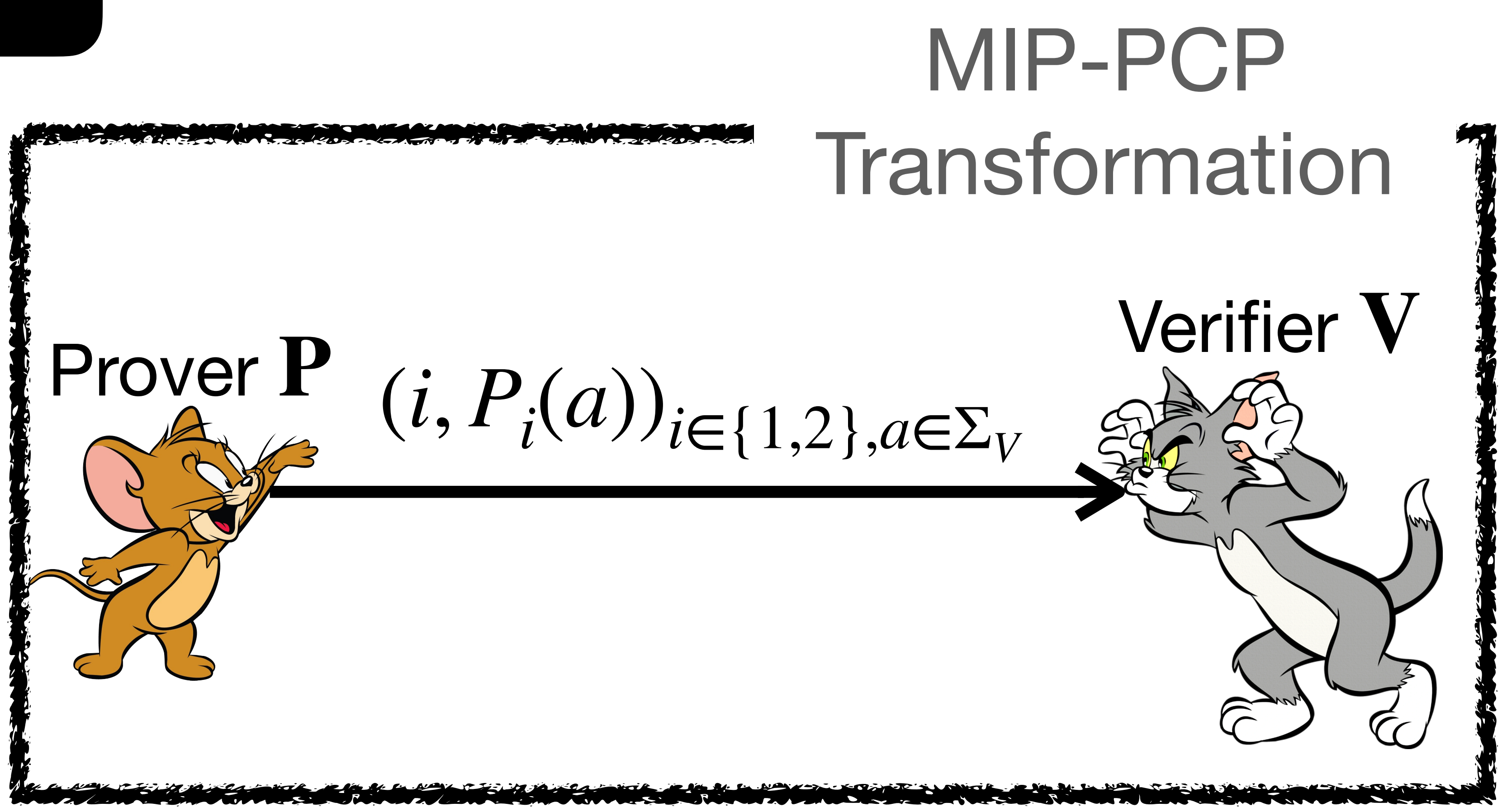
NP-complete language $\xrightarrow{\text{PCP theorem}}$ PCP $\xrightarrow{\text{PCP-MIP Transformation}}$ 2-prover MIP

Step 2. Parallel repeat the 2-prover MIP to reduce soundness error.

2-prover MIP $\xrightarrow{\text{Parallel repetition}}$ Low error 2-prover MIP

Step 3. Convert the repeated MIP back to a PCP.

Low error 2-prover MIP $\xrightarrow{\text{MIP-PCP Transformation}}$ PCP′



Parallel repetition for PCPs fails

Parallel repetition for PCPs fails

Theorem 1.

2-query PCP
for NP-complete language L
soundness error $\beta < 1$

$\xrightarrow{\text{t-wise parallel repetition}}$

2-query PCP for L
soundness error β_t

for every $x \notin L$, $\lim_{t \to \infty} \beta_t = 1$

In particular, $\beta(x)^t \leq \beta_t(x) \leq \beta(x)$ does not hold.

PCP for 3COL

- 3COL := $\{G : G$ has a 3-coloring$\}$
- PCP = $(\mathbf{P}, \mathbf{V})$ for 3COL

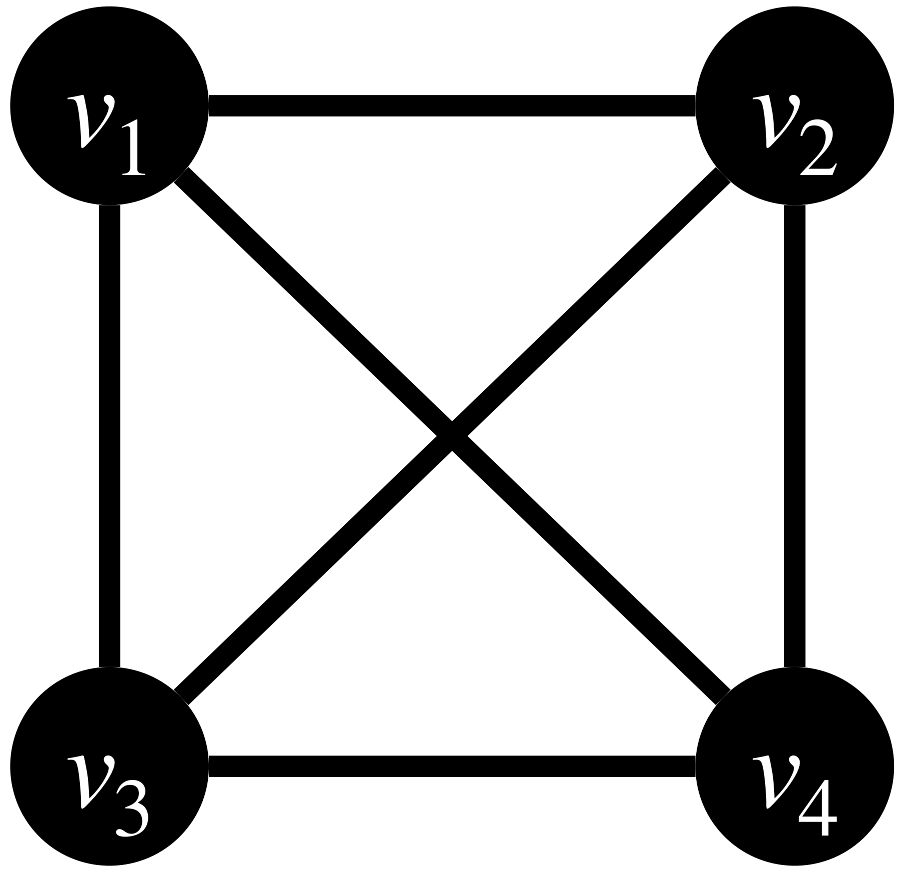
$\pi : V \to \{0,1,2\}$

Verifier $\mathbf{V}\left(G = (V, E)\right)$

1. Sample $\{u, v\} \leftarrow E$. _(Assume $u < v$.)_
2. Query π at u and v, and check that $\pi[u] \neq \pi[v]$.

- Perfect completeness: $\mathbf{V}$ always accepts for every $G \in$ 3COL.
- Soundness: $\beta(G) \leq \dfrac{|E| - 1}{|E|}$ for every $G \notin$ 3COL.

Parallel repetition for PCP for $3\mathsf{COL}$ fails [1/2]



Second position in $\mathbf{V}_2$'s query

First position in $\mathbf{V}_2$'s query

$\tilde{\Pi}$	v_1	v_2	v_3	v_4
v_1	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
v_2	$(0,0)$	$(1,1)$	$(1,1)$	$(1,1)$
v_3	$(0,0)$	$(1,1)$	$(1,1)$	$(1,1)$
v_4	$(0,0)$	$(1,1)$	$(1,1)$	$(1,1)$

Verifier $\mathbf{V}_2$

- $\mathbf{V}_2$ rejects if and only if answers to both queries are $(1,1)$:
  - Why can't it happen when both answers are $(0,0)$?
  - Both answers are $(1,1)$ if and only if v_1 is not queried.
- Soundness error: $\beta_2(K_4) \geq 1 - \left(\frac{3}{6}\right)^2 = \frac{3}{4}$.

- $\mathbf{V}$'s query lists: $Q_1 = (u_1, w_1)$, $Q_2 = (u_2, w_2)$.
- $\mathbf{V}_2$'s queries: $\mathbf{Q}_1 = (u_1, u_2)$, $\mathbf{Q}_2 = (w_1, w_2)$.
  - $u_1 < w_1$ and $u_2 < w_2$.
  - Answer to $\mathbf{Q}_2$ cannot be $(0,0)$.

Parallel repetition for PCP for $3\mathsf{COL}$ fails [2/2]

Malicious prover strategy

For every possible query (q_1, q_2) of $\mathbf{V}_2$:

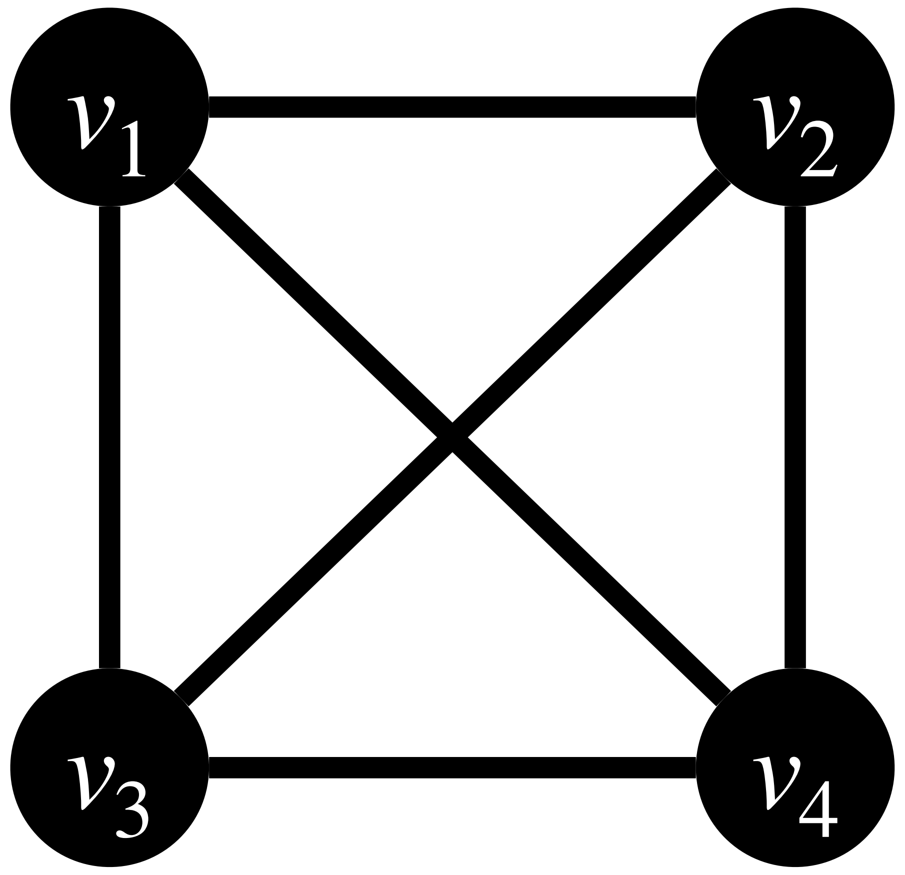
- If at least one of (q_1, q_2) is the smallest non-isolated vertex in G: Set $\tilde{\Pi}[(q_1, q_2)] = (0,0)$.
- Otherwise, Set $\tilde{\Pi}[(q_1, q_2)] = (1,1)$.

$$\implies \beta_2(G) \geq 1 - \left(\frac{|E| - 1}{|E|}\right)^2.$$

t-wise parallel repetition: $\beta_t(G) \geq 1 - \left(\frac{|E| - 1}{|E|}\right)^t$

$$\implies \lim_{t \to \infty} \beta_t(G) = 1.$$

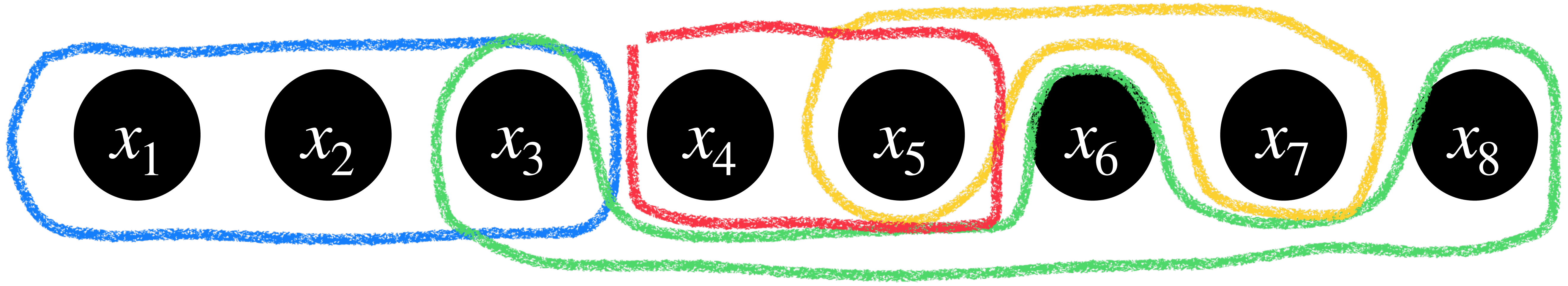
Parallel repetition for PCP increases soundness error



- $\beta(K_4) \leq \frac{5}{6}$
- $\beta_2(K_4) \geq \frac{3}{4}$
- $\beta_2(K_4) > \beta(K_4)$

In general, we can show that there are infinitely many instances $G \notin$ 3COL such that $\beta_t(G) > \beta_{t-1}(G)$.

Generalization to symmetric CSPs [1/2]

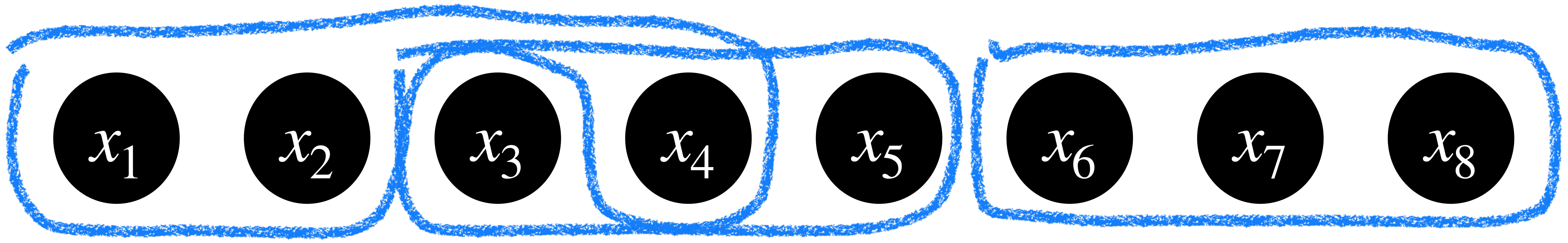


Constraint satisfaction problem (CSP):

- A list ϕ of constraints over variables in X.
- Each constraint checks a predicate f over some variables.
- ϕ is satisfiable if and only if there is an assignment to the variables that satisfies all constraints.

$\Longrightarrow$ 3COL is a CSP: each constraint is over an edge and checking the vertex colors.

3COL is a **symmetric CSP**: the predicate for each constraint is the same.



Generalization to symmetric CSPs [2/2]

Lemma 1.

randomly selects a constraint and check its satisfiability

PCP
for symmetric CSP
soundness error β

t-wise
parallel repetition

PCP$_t$
soundness error β_t

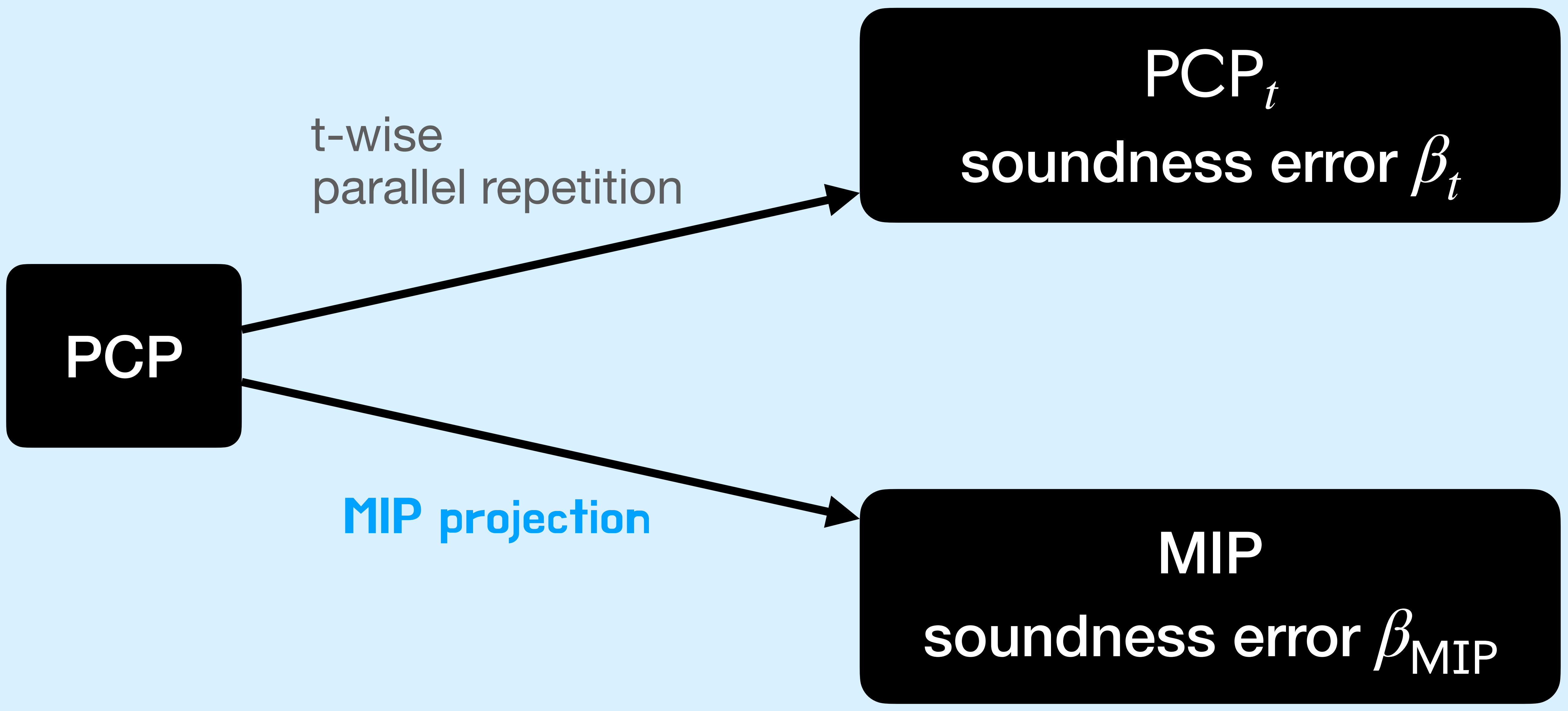
for every $t \in \mathbb{N}$, $\beta_{t+1} \geq \beta_t$ and $\beta > 0 \implies \lim_{t \to \infty} \beta_t > 0$

Note: Lemma 1 does not extend to non-symmetric CSPs. e.g. 3SAT is a non-symmetric CSP, we show that for some instances for 3SAT, $\beta > 0$ and $\lim_{t \to \infty} \beta_t = 0$.

A characterization result

The characterization result

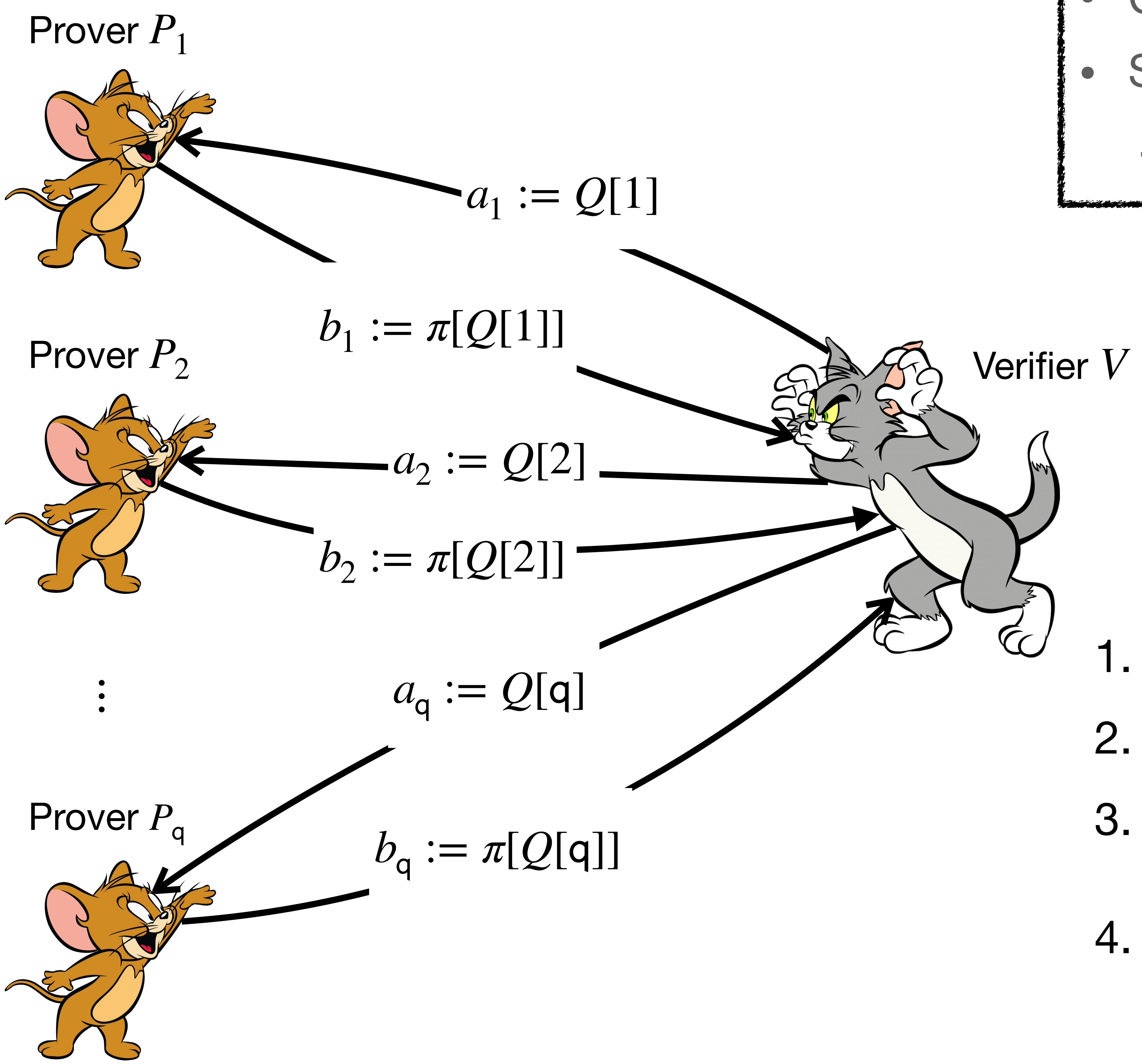
Theorem 2.



for every $x \notin L$, $\lim_{t\to\infty} \beta_t = 0 \iff \beta_{\mathrm{MIP}} < 1$

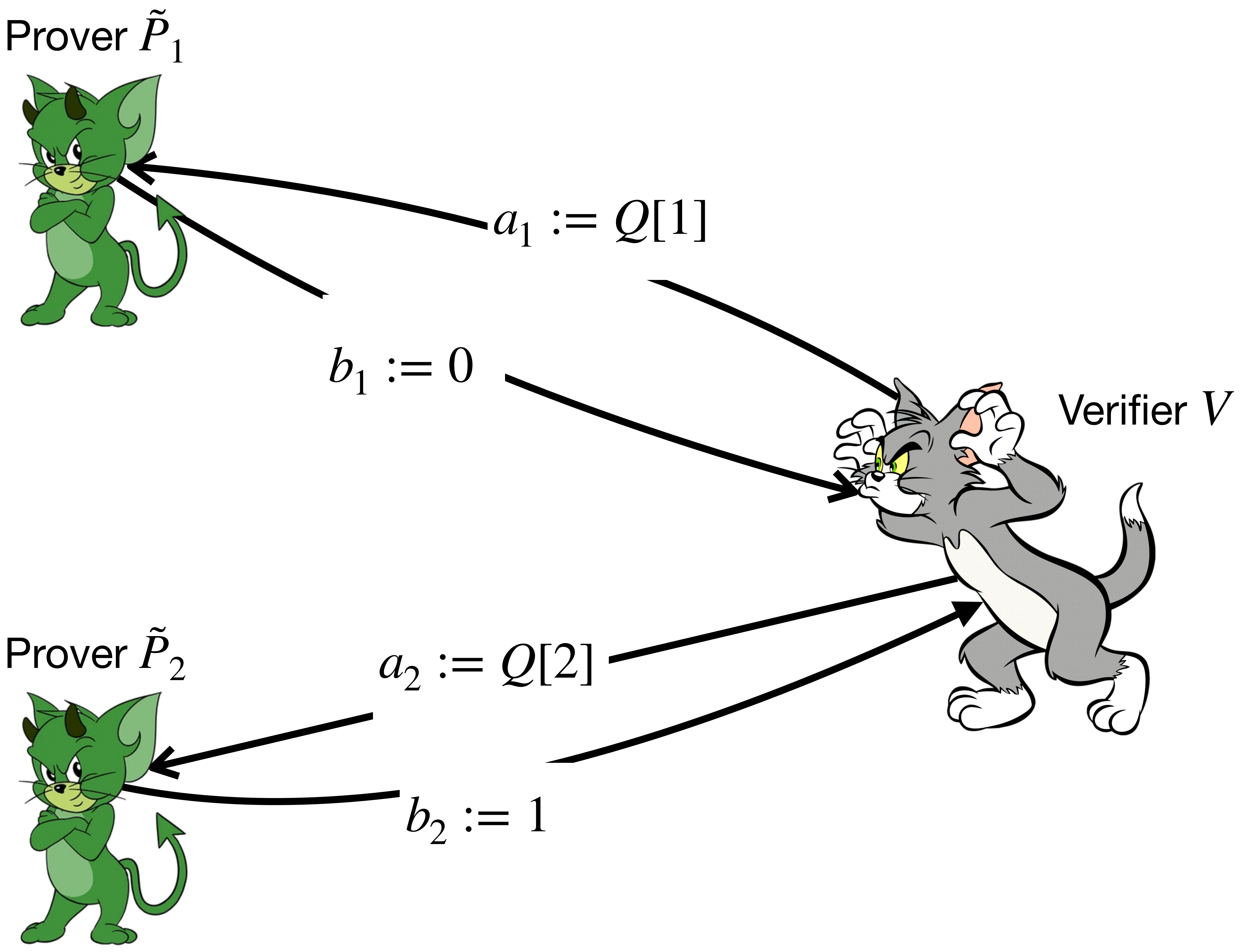
MIP projection

- Completeness of the MIP is the same as that of PCP.
- Soundness: for every $x \notin L$, $\beta_{\text{MIP}}(x) \geq \beta_{\text{PCP}}(x)$.
  - No consistency check $\Longrightarrow$ MIP might not be secure.



1. Sample a randomness for $\mathbf{V}$: $\rho \leftarrow \{0,1\}^\mathsf{r}$.
2. Compute query lists of $\mathbf{V}$: $Q := \mathbf{V}_q(x; \rho)$.
3. Send the i-th query to the i-th prover P_i and get their replies.
4. Check that $\mathbf{V}$ accept: $\mathbf{V}_d\left(x, \rho, (b_i)_{i \in [\mathsf{q}]}\right)$.

Revisit: parallel repetition for PCP for 3COL



Theorem 2. $\lim_{t\to\infty} \beta_t = 0 \iff \beta_{\mathrm{MIP}} < 1$

$\implies \beta_{\mathrm{MIP}} = 1$ for 3COL.

- First malicious MIP prover always send 0.
- Second malicious MIP prover always send 1.

Proof of Theorem 2 [1/2]

$$\beta_{\mathsf{MIP}} = 1 \implies \lim_{t\to\infty} \beta_t \geq \frac{1}{2^{\mathsf{r}}} > 0$$

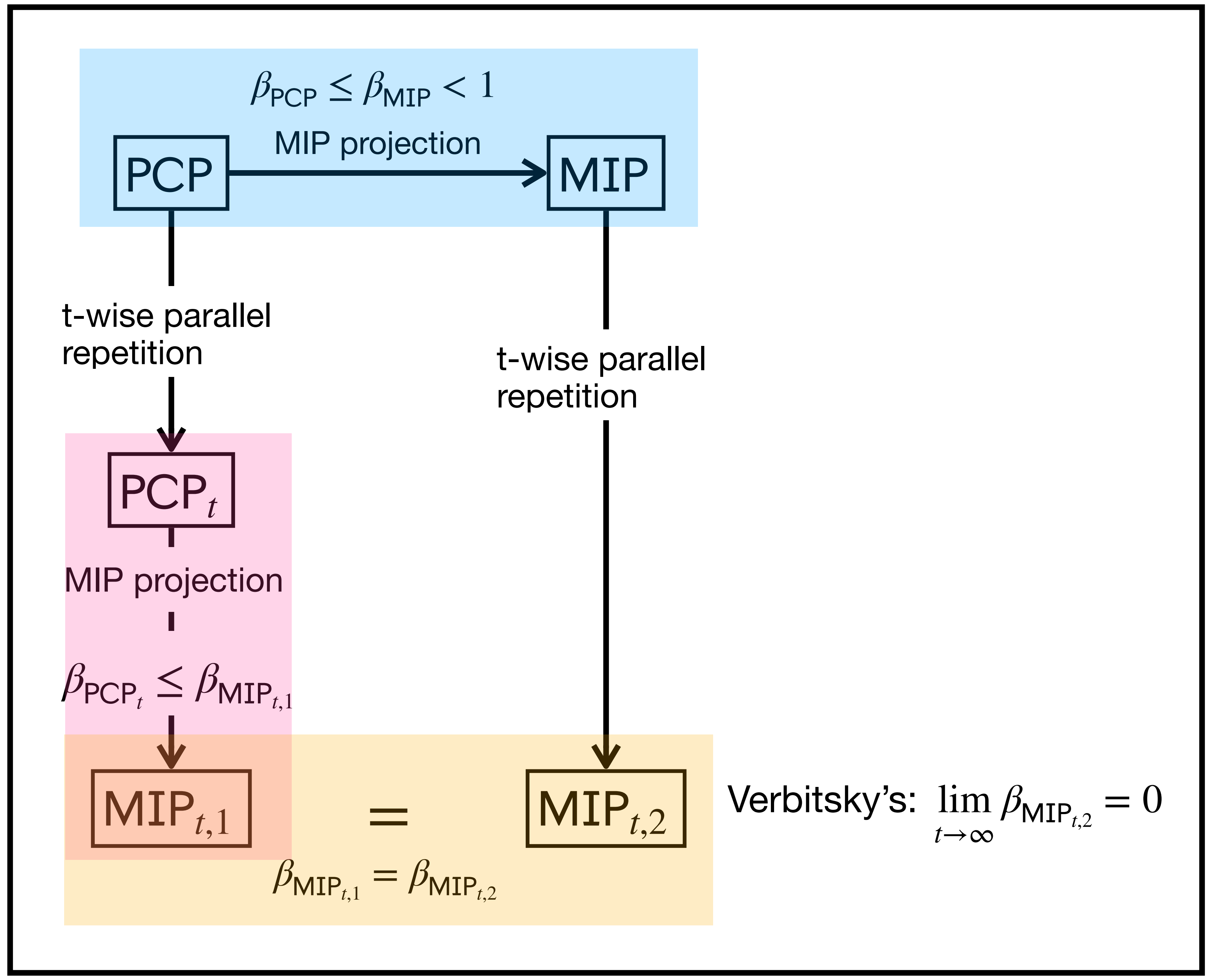
- The optimal MIP provers can always convince the MIP verifier.
  - Moreover, we can find $(2^r)^{t-1}$ different randomness ρ such that $\mathbf{V}_t(\rho)$ can be convinced.
- $\beta_t(x) \geq \dfrac{|W_{t,\rho^\star}|}{|(\{0,1\}^{\mathsf{r}})^t|} = \dfrac{(2^{\mathsf{r}})^{t-1}}{(2^{\mathsf{r}})^t} = \dfrac{1}{2^{\mathsf{r}}} \implies \lim_{t\to\infty} \beta_t(x) = \dfrac{1}{2^{\mathsf{r}}}.$

Note: We show the above analysis is tight by giving examples of PCPs whose limits attain $\dfrac{c}{2^{\mathsf{r}}}$ for every $c \in [1,2^{\mathsf{r}}]$.

Proof of Theorem 2 [2/2]

$$\beta_{\mathsf{MIP}} < 1 \implies \lim_{t\to\infty} \beta_t = 0$$

- Key observation: MIP projection and parallel repetition **commutes**.
- i.e. The MIP projection of the parallel repetition for PCP is equivalent to the parallel repetition of the MIP projection of the PCP.

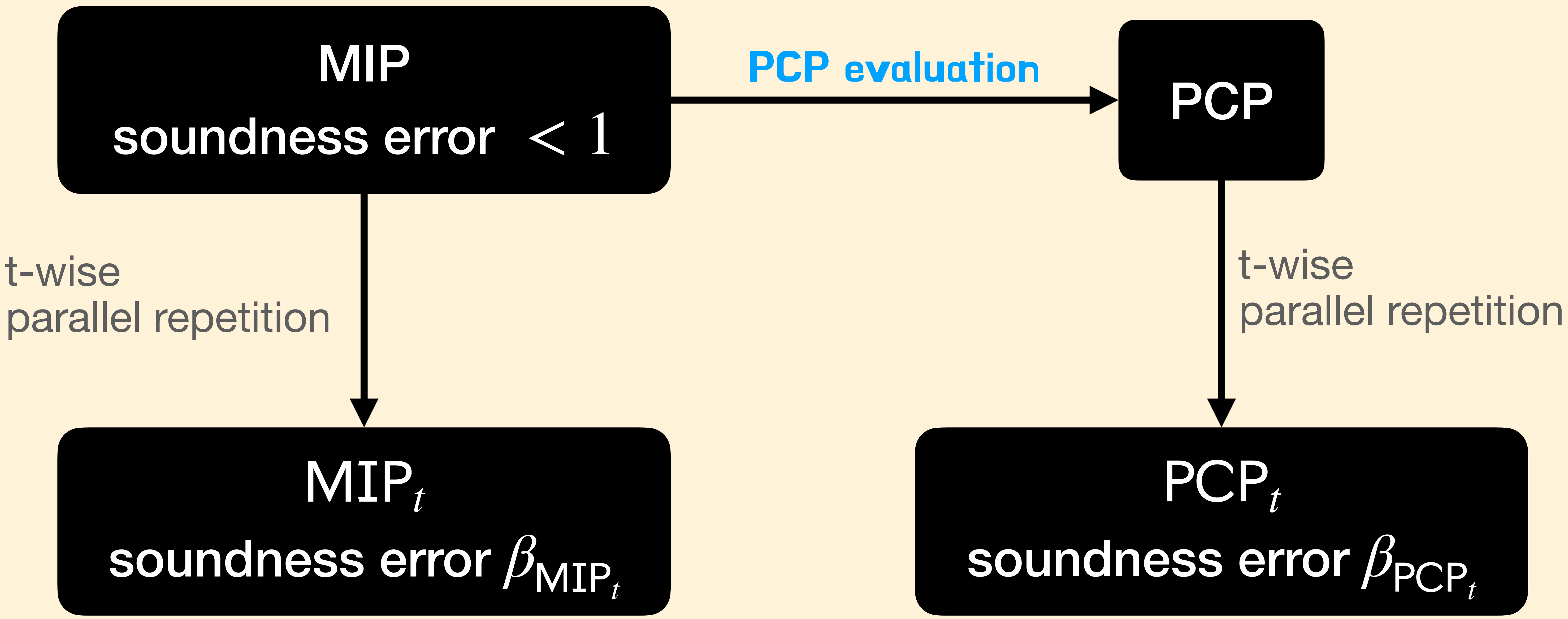


$$\implies \lim_{t\to\infty} \beta_{\mathsf{PCP}_t} = 0$$

Rate of decay of parallel repetition

Rate of decay of parallel repetition

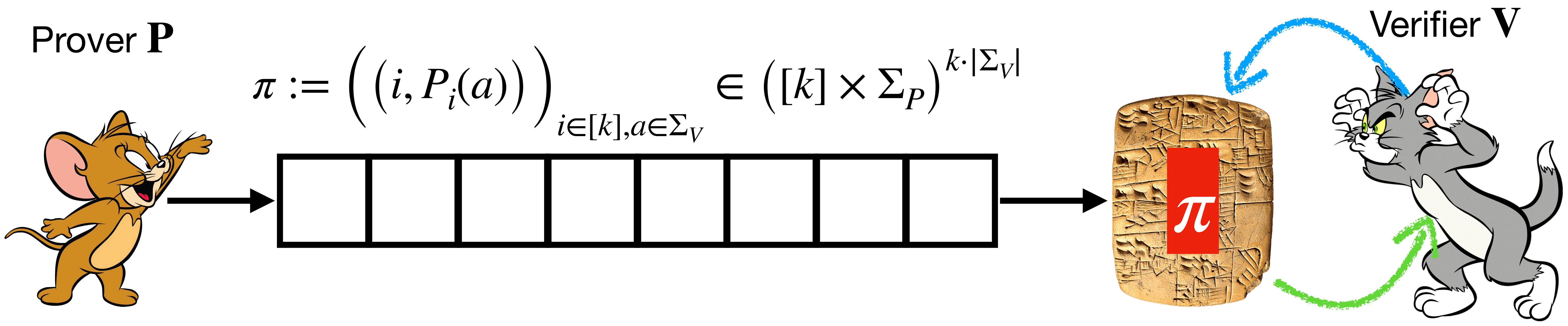
Lemma 2.

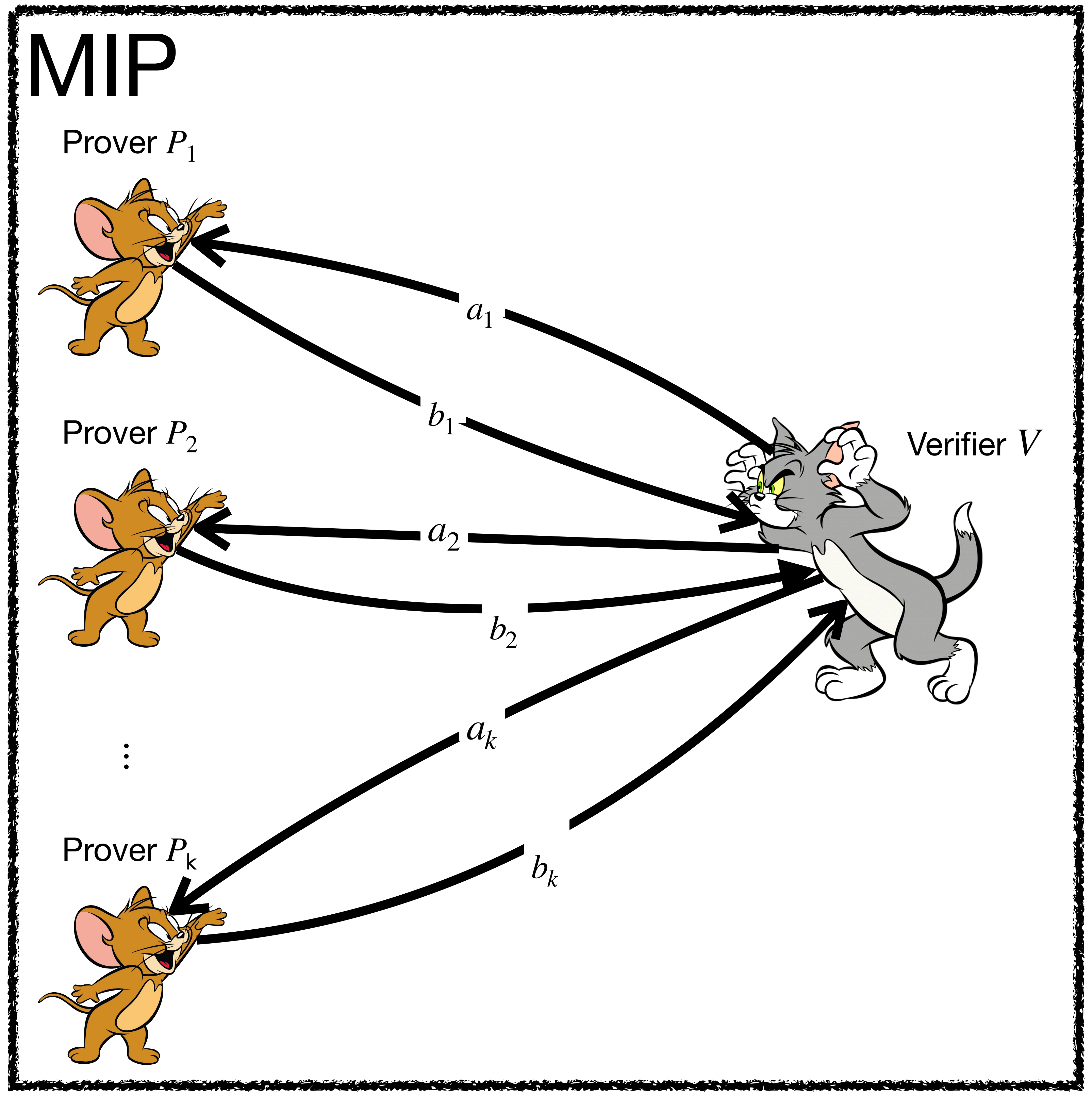


for every $x \notin L$ and $t \in \mathbb{N}$, $\beta_{\text{PCP}_t}(x) = \beta_{\text{MIP}_t}(x) < 1$

PCP evaluation

$\pi \in \Sigma^l$

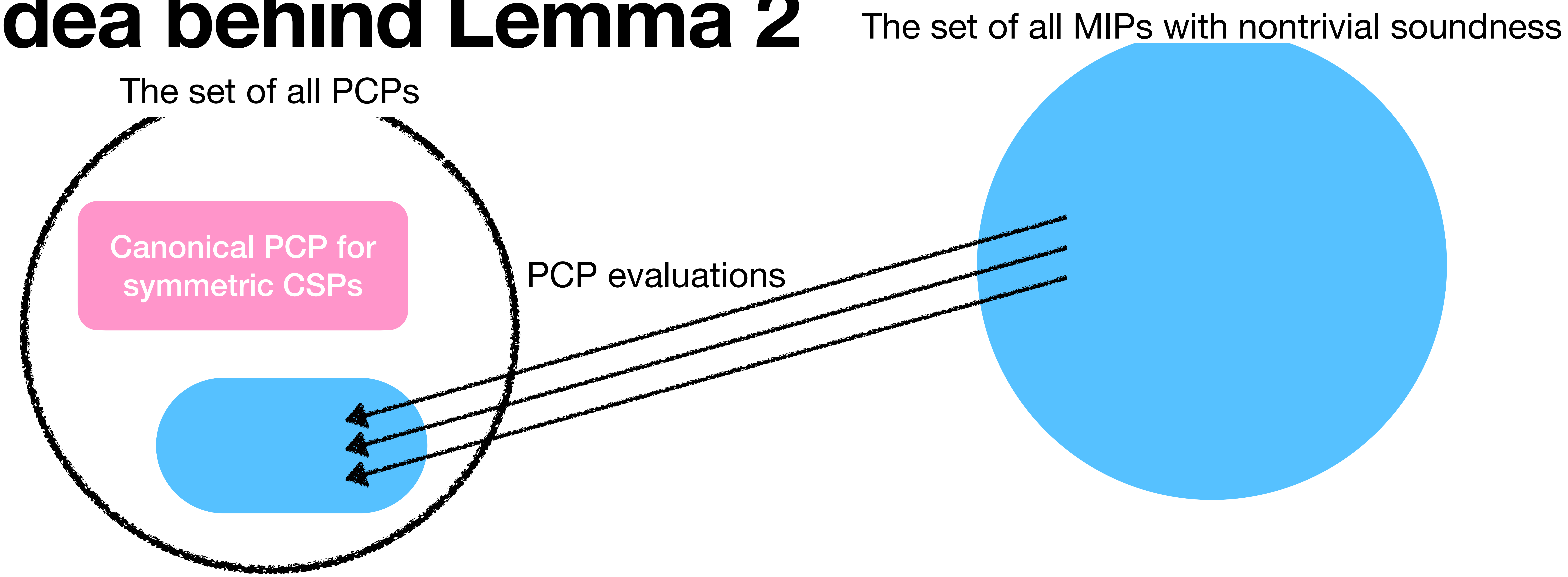


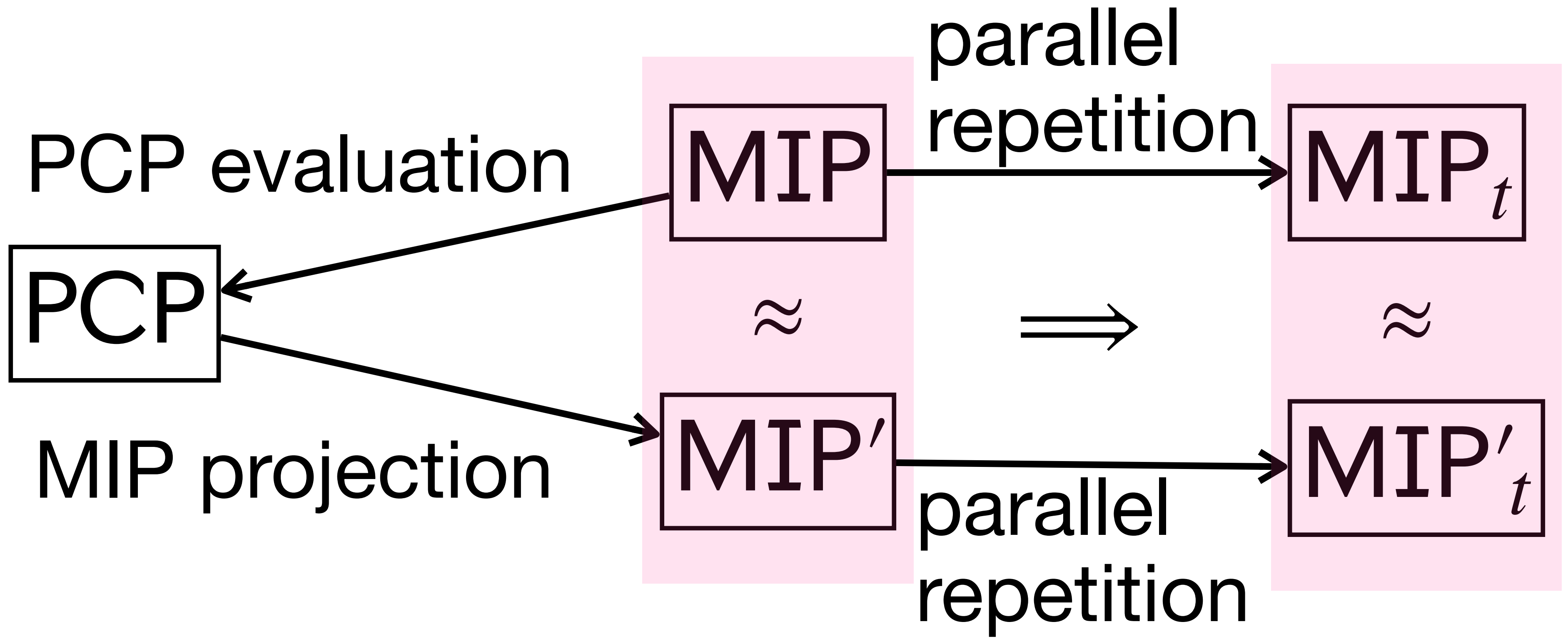


Completeness and soundness of the PCP are the same as that of the MIP.

Theorem 2 (characterization) tells us: if $\beta_{\text{MIP}} < 1$, parallel repetition works for its PCP evaluation!

Idea behind Lemma 2



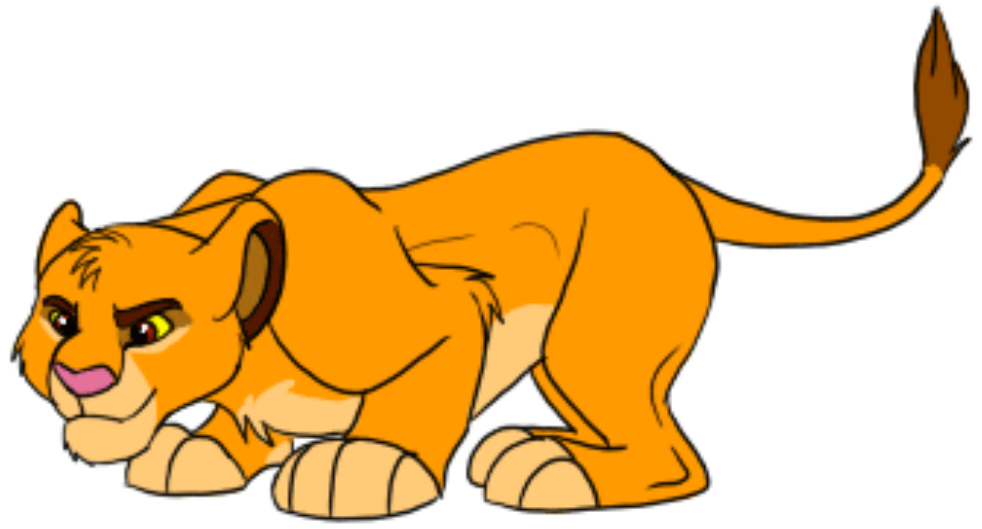


$\Longrightarrow$ $\beta_{\mathrm{PCP}_t} \leq \beta_{\mathrm{MIP}_t} < 1$

$\beta_{\mathrm{PCP}_t} \geq \beta_{\mathrm{MIP}_t}$ (proved by construct malicious PCP strategy from MIP strategy)

$\Longrightarrow$ $\beta_{\mathrm{PCP}_t} = \beta_{\mathrm{MIP}_t} < 1$

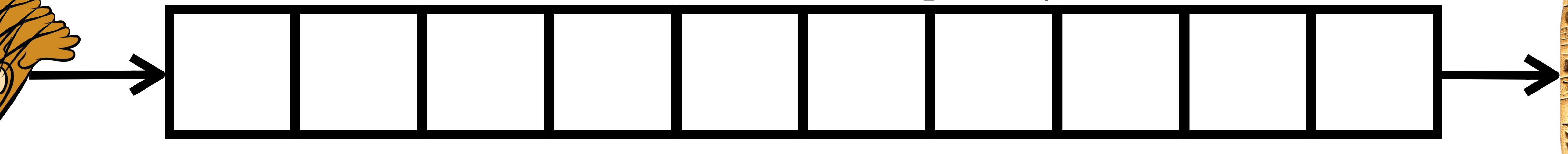
Consistent parallel repetition works



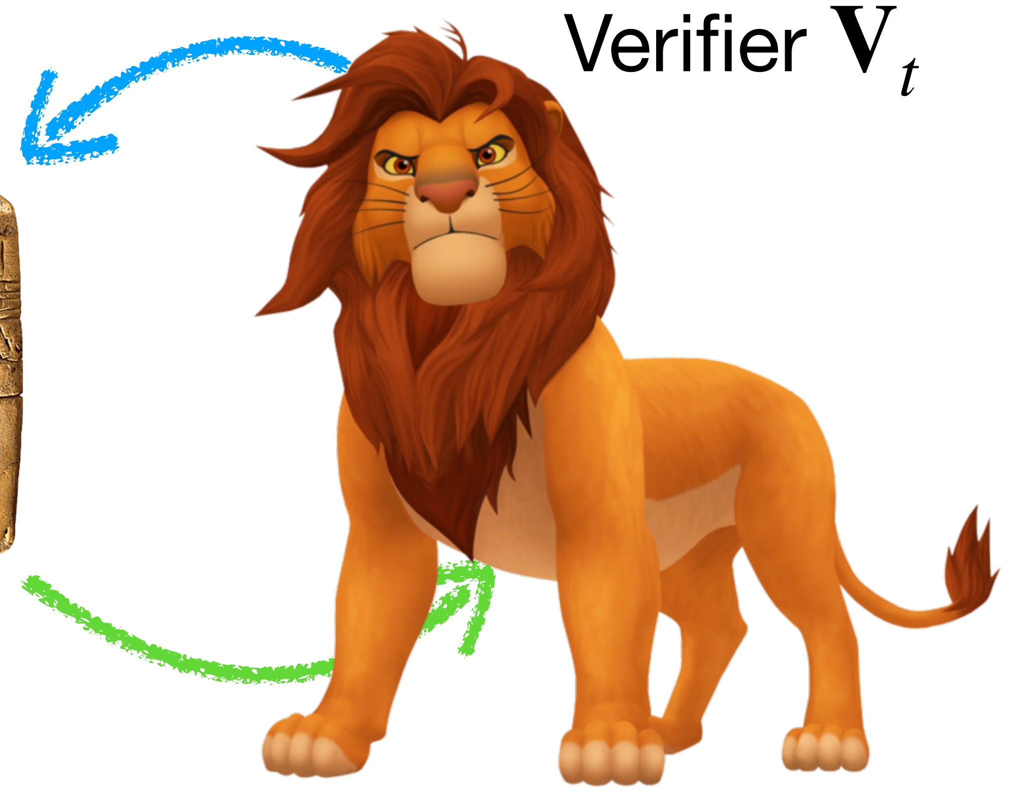
Solution: consistent parallel repetition [1/3]

Prover $\mathbf{P}_t$

$\Pi := ((\pi[q_1], \ldots, \pi[q_t]))_{(q_1,\ldots,q_t)\in[l]^t} \in \left(\Sigma^t\right)^{l^t}$

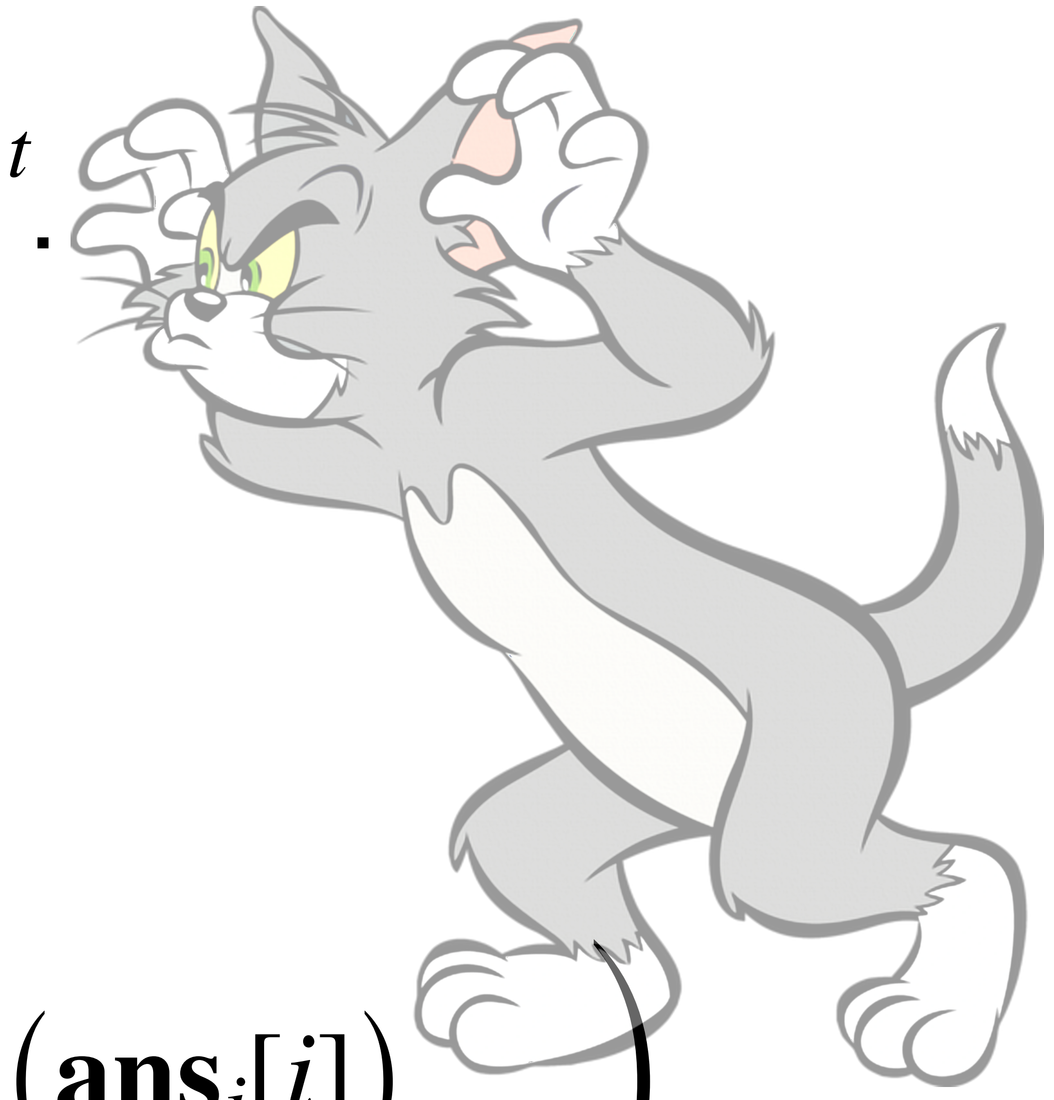


Verifier $\hat{\mathbf{V}}_t$



No additional queries or randomness compare to parallel repetition!

1. Sample t randomness for $\mathbf{V}$: $(\rho_i)_{i\in[t]} \leftarrow \left(\{0,1\}^{\mathsf{r}}\right)^t$.
2. Compute query lists of $\mathbf{V}$: $Q_i := \mathbf{V}_q(x;\rho_i)$.
3. Compute query lists of $\hat{\mathbf{V}}_t$: $\mathbf{Q}_i := \left(Q_j[i]\right)_{j\in[t]}$.
4. Query the PCP string Π: $\mathbf{ans}_i := \Pi[\mathbf{Q}_i]$.
5. Check that for every repetition $i \in [t]$: $\mathbf{V}_d\left(x, \rho_i, \left(\mathbf{ans}_j[i]\right)_{j\in[\mathsf{q}]}\right)$.
6. For every query $q \in [l]$ made by $\hat{\mathbf{V}}_t$, if it is queried more than once, check that all answers to q are the same.



Solution: consistent parallel repetition [2/3]

Theorem 3.

PCP
soundness error $\beta < 1$

t-wise
consistent parallel repetition

$\longrightarrow$

PCP$_t$
soundness error $\hat{\beta}_t$

for every $x \notin L$ and $t \in \mathbb{N}$, $\hat{\beta}_t(x) \leq O_x(1) \cdot \beta(x)^t$

$$O_x(1) \leq \binom{2^{\mathrm{r}}}{\beta(x) \cdot 2^{\mathrm{r}}}$$

Solution: consistent parallel repetition [3/3]

$O_x(1)$ is a large constant that doesn't depend on t.

- Derived from a counting problem:

$$\mathscr{K}(\Sigma, n, m) := \left| \left\{ s = (s_1, \ldots, s_n) \in \Sigma^n : |\{s_1, \ldots, s_n\}| \leq m \right\} \right|.$$

- Bounded from the above by $\binom{|\Sigma|}{m} \cdot m^n$.

- Open problem: can $O_x(1)$ be improved?

Future directions

Question 1. Can we replace the dichotomy in the characterization result by a trichotomy?

- Three behaviors of parallel repetition: Limit doesn't go to 0, limit goes to 0, and soundness error strictly increases after each repetition.

Question 2. More precise rate of decay of parallel repetition?

- Direct analysis without mentioning MIPs?

Question 3. Is there more to say about rate of decay of consistent parallel repetition?

- Better constant?
- Another curve?

Thank you!

https://eprint.iacr.org/2023/1714