Title: Binary constraint systems and MIP*

Speakers: William Slofstra

Collection: Foundations of Quantum Computational Advantage

Date: May 02, 2024 - 1:00 PM

URL: https://pirsa.org/24050012

Abstract: Binary constraint system games are a generalization of the Mermin-Peres magic square game introduced by Cleve and Mittal. Thanks to the recent MIP*=RE theorem of Ji, Natarajan, Vidick, Wright, and Yuen, BCS games can be used to construct a proof system for any language in MIP*, the class of languages with a multiprover interactive proof system where the provers can share entanglement. This means that we can apply logical reductions for binary constraint systems to MIP* protocols, and also raises the question: how complicated do our constraint systems have to be to describe all of MIP*? In this talk, I'll give a general overview of this subject, including an application of logical reductions to showing that all languages in MIP* have a perfect zero knowledge proof system (joint work with Kieran Mastel), and one obstacle to expressing all of MIP* with linear constraints (joint work with Connor Paddock).

## I Mermin-Peres magic square

$$\begin{array}{|c|c|c|c}
x_1 & x_2 & x_3 & 0 \\
\hline
x_4 & x_5 & x_6 & 0 \\
\hline
x_7 & x_8 & x_9 & 0 \\
\hline
1 & 1 & 1 &
\end{array}$$

$$\left.\begin{aligned}
x_1+x_2+x_3&=0\\
x_4+x_5+x_6&=0\\
&\vdots\\
x_3+x_6+x_9&=1
\end{aligned}\right\}\ \text{6 eq'ns}$$

System has no sol'n in $\mathbb{Z}_2$.

We can assign unitary matrices $X_1, \ldots, X_9$ to the entries s.t.

(1) $X_i^2 = 1$

(2) product across rows is $\mathbb{1}$, product across columns is $-\mathbb{1}$

(3) $X_i X_j = X_j X_i$ if are in the same column.

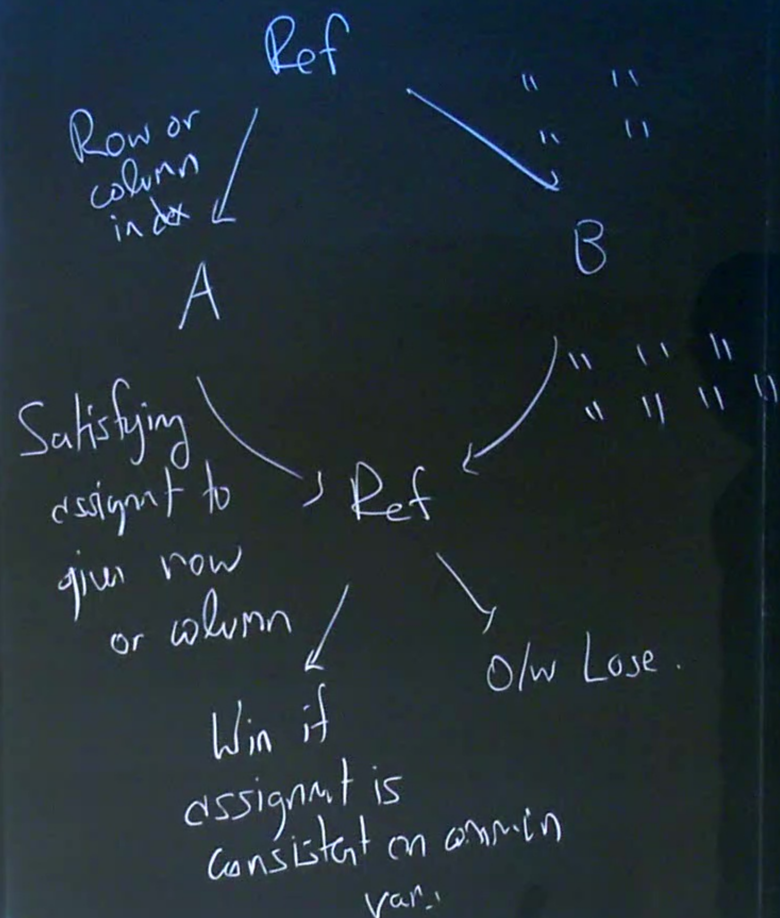
Quantum satisfying

(3) $X_i X_j = X_j X_i$ if $X_i, X_j$ are in the same row or column.

Quantum satisfying assignment

Operators $\Rightarrow$ contextuality.

## II MP game



$= X_j X_i$ if $X_i X_j$

the same row or

satisfying assignment

$\Rightarrow$ contextuality.

## II MP game

Ref

Row or column index

A

no commun.

B

"   "

Satisfying assignmt to given row or column

Ref

Win if assignment is consistent on common var.

O/w Lose.

Not possible to play perfectly w/ classical resources.

However, they can turn any q satisfying assignmt if a perfect strategy using entanglement.

## III. Binary constraint system

game

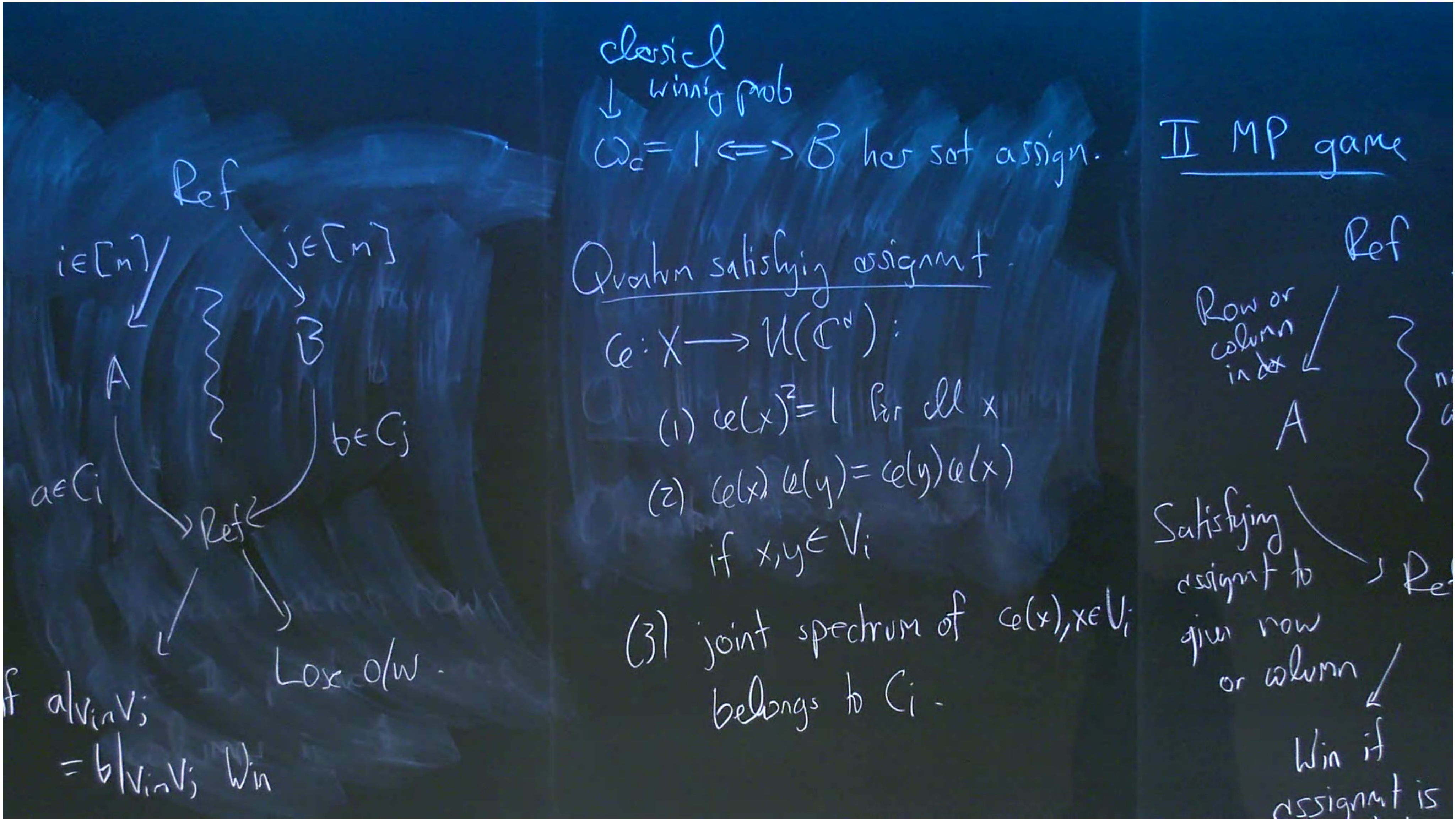
$B = X$ set of vars

$\{(V_i, C_i)\}_{i=1}^{m}$

$V_i \subseteq X$, $C_i \subseteq \mathbb{Z}_2^{V_i}$ satisfying assignments

$$\begin{tikzcd}
 & \mathrm{Ref} \arrow[dl, "i \in [m]"'] \arrow[dr, "j \in [m]"] & \\
A \arrow[dr, bend right, "a \in C_i"'] & & B \arrow[dl, bend left, "b \in C_j"] \\
 & \mathrm{Ref} \arrow[dl] \arrow[dr] & \\
W & & \text{Lose o/w.}
\end{tikzcd}$$

if $a|_{V_i \cap V_j} = b|_{V_i \cap V_j}$ Win


Ref
$i \in [n]$
$j \in [n]$
A
B
$a \in C_i$
$b \in C_j$
Ref
Lose o/w.
if $a|_{V_i \cap V_j} = b|_{V_i \cap V_j}$ Win
classical
winning prob
$\omega_c = 1 \iff B$ has sat assign.
Quantum satisfying assignment
$\mathcal{C}: X \longrightarrow \mathcal{U}(\mathbb{C}^d)$:
(1) $\mathcal{C}(x)^2 = 1$ for all $x$
(2) $\mathcal{C}(x)\mathcal{C}(y) = \mathcal{C}(y)\mathcal{C}(x)$ if $x, y \in V_i$
(3) joint spectrum of $\mathcal{C}(x), x \in V_i$ belongs to $C_i$.
II MP game
Ref
Row or column index
A
Satisfying assignment to given row or column
Win if assignment is

B has sat assign.

ing assignment

$(\mathbb{C}^d)$:

$= 1$ for all $x$

$(y) = \omega(y)\omega(x)$

$y \in V_i$

spectrum of $\omega(x), x \in V_i$

ngs to $C_i$.

Q sat assignment in $\mathcal{U}(\mathbb{C}^d)$

$\Rightarrow$ perfect q strat w/

$|\psi_{max}\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$

$\omega_q = \sup_d$ of winning prob w/

q strats in $\mathbb{C}^d \otimes \mathbb{C}^d$

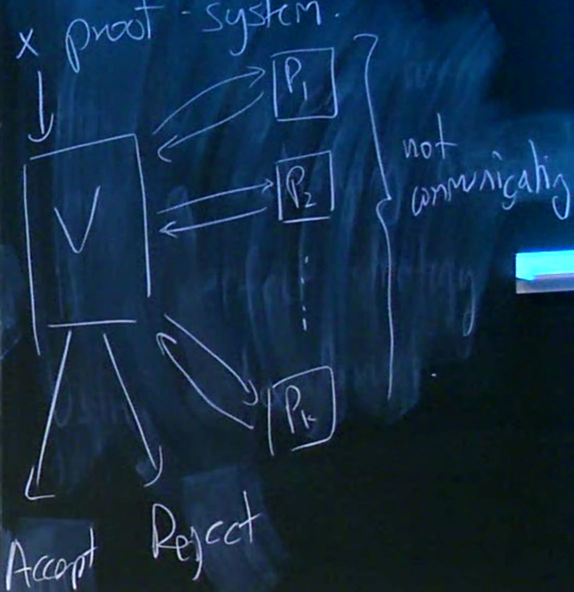
$\omega_q = 1 \iff$ q sat assignment

in $\mathcal{U}(R^\omega) \leftarrow$ hyperfinal

$II_1$ factor

## IV MIP*

MIP = multiprover interactive proof system.



$\{0,1\}^* \cup$

A language $\mathcal{L}$ is in MIP if there is a verifier V s.t.

(1) if $x \in \mathcal{L}$, then there is a way for the provers to convince V to accept (w/ prob = 1)

(2) if $x \notin \mathcal{L}$, the prob(accept) $< 1-s$ for all possible actions by the provers.

Ref

$i \in [n]$ → A

$j \in [n]$ → B

A → Ref: $a \in C_i$

B → Ref: $b \in C_j$

Ref → $a|_{V_i \cap V_j} = b|_{V_i \cap V_j}$ Win

Ref → Lose o/w.

classical

winning prob

$\omega_c = 1 \iff \mathcal{B}$ has

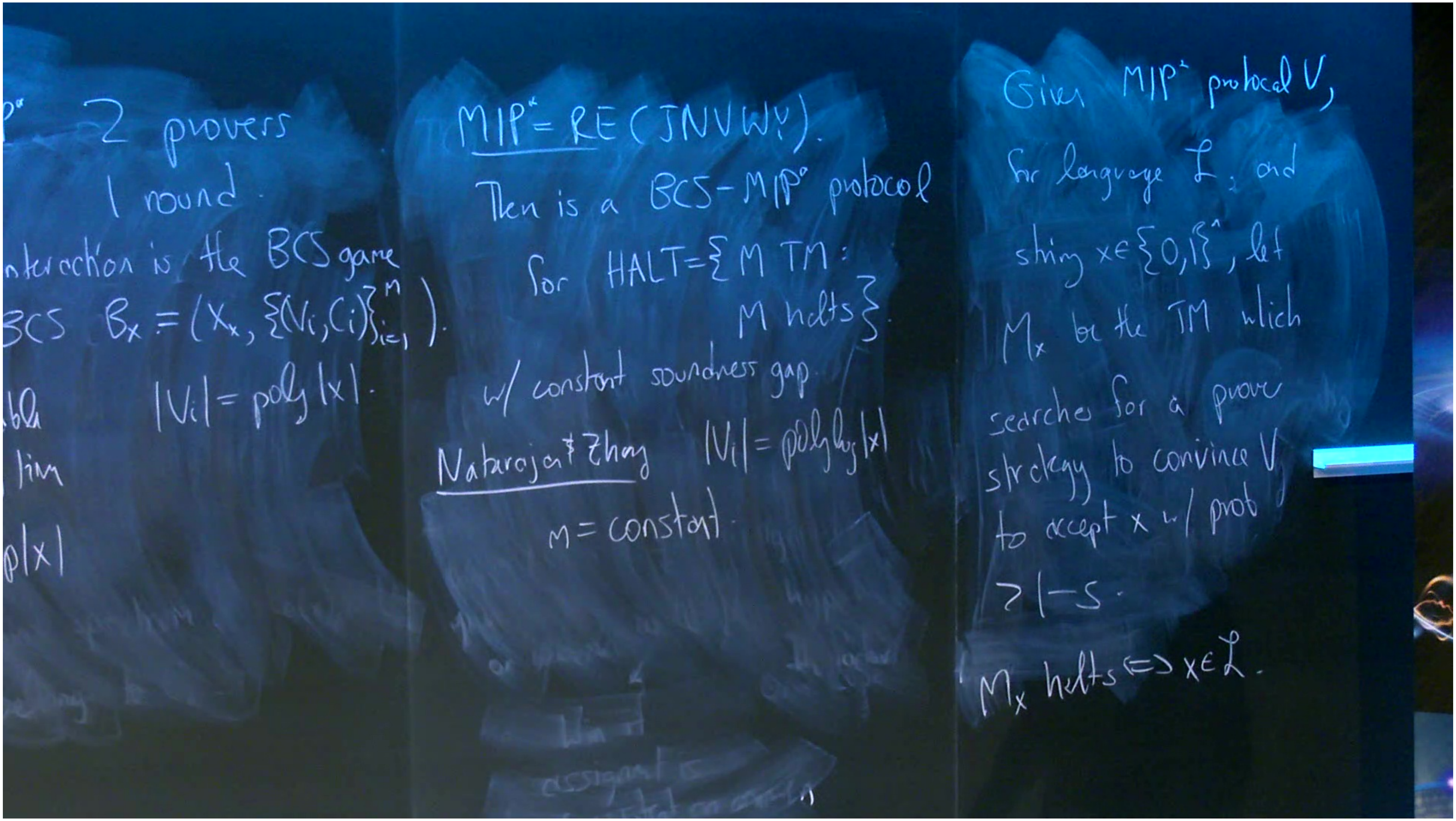
Quantum satisfying assig

$\mathcal{C}: X \longrightarrow \mathcal{U}(\mathbb{C}^d)$:

(1) $\mathcal{C}(x)^2 = 1$ for

(2) $\mathcal{C}(x)\,\mathcal{C}(y) = \mathcal{C}(y$
if $x, y \in V_i$

(3) joint spectrum belongs to $C_i$


2 provers
1 round.
nteraction is the BCS game
BCS $B_x = (X_x, \{(V_i, C_i)\}_{i=1}^{m})$.
$|V_i| = \text{poly}|x|$.
lim
p|x|
MIP* = RE (JNVWY).
Then is a BCS-MIP* protocol
for HALT = {M TM : M halts}.
w/ constant soundness gap.
Natarajan & Zhang
$|V_i| = \text{polylog}|x|$
$m = \text{constant}$.
Given MIP* protocol V,
for language $\mathcal{L}$, and
string $x \in \{0,1\}^n$, let
$M_x$ be the TM which
searches for a prover
strategy to convince V
to accept x w/ prob
$\geq 1-s$.
$M_x$ halts $\iff x \in \mathcal{L}$.

PERIMETER INSTITUTE FOR THEORETICAL P

We can understand all of MIP* using BCS-MIP*.

## V Logical reductions

Ex Given a constraint $C$ on vars $V$, we can add new vars $W \supseteq V$ and rewrite $C$ as a 3SAT instance $D$ on $W$ s.t. $\varphi \in C \Leftrightarrow \exists \psi \in D$ s.t. $\psi|_V = \varphi$.

Prop (Mastel-S) Reductions like this do not change the soundness gap.

BCS-MI

Every i

of a B

$C_i$ checkab

in poly

$m = \exp$

uctions

...strent C on vars V,

...ew vars $W \supseteq V$

C is a 3SAT

W s.t. $\varphi \in C \iff$

$\psi|_V = \varphi$.

) Reductions like this change the soundness

...p.

$x_1 \vee x_2 \vee x_3 \wedge x_1 \vee x_4 \vee x_5$.

on $x_1, \dots, x_5$. $\quad x_2x_5 = x_5x_2$

VS $x_1 \vee x_2 \vee x_3$ on $\{x_1, x_2, x_3\}$ and $x_1 \vee x_4 \vee x_5$ on $\{x_1, x_4, x_5\}$

$x_2x_5 \neq x_5x_2$.

Prop Good splitting $\Rightarrow$ soundness gap does not drop off too badly.

Ex $MIP^* \subseteq 3SAT\text{-}MIP^*$ w/ poly gap.

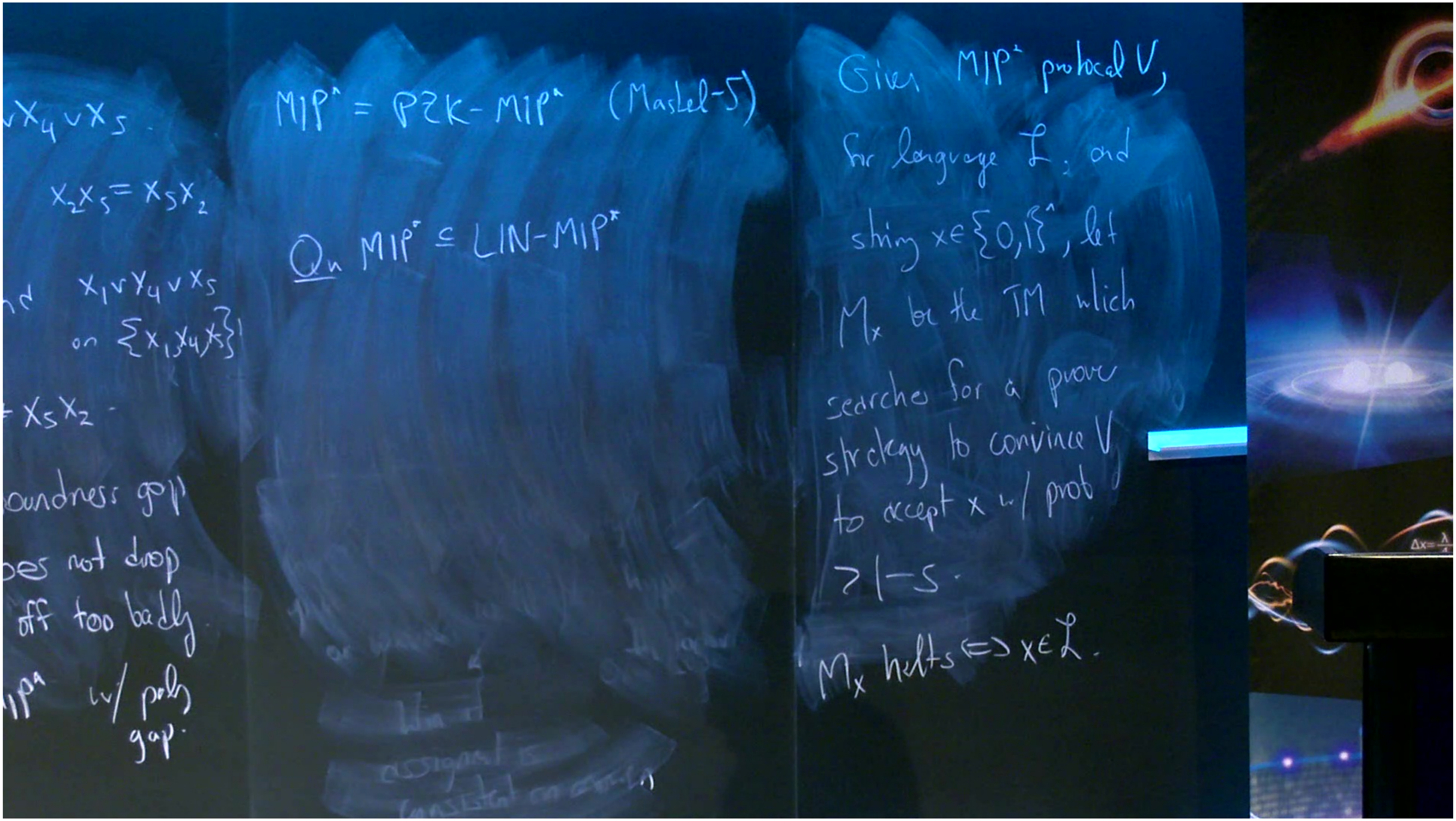
$MIP^* = RE$ (JNVWY).

Then is a BCS-$MIP^*$ protocol for HALT = {M TM : M halts}.

w/ constant soundness gap.

Natarajan & Zhang $\quad |V_i| = \mathrm{poly}\log|x|$

$m$ = constant.


$\vee X_4 \vee X_5$.
$X_2X_5 = X_5X_2$
nd $X_1 \vee X_4 \vee X_5$
on $\{X_1, X_4, X_5\}$
$= X_5X_2$.
oundness gap
oes not drop
off too badly.
$IP^*$ w/ poly gap.
$MIP^* = PZK\text{-}MIP^*$ (Mastel-S)
Q: $MIP^* \subseteq LIN\text{-}MIP^*$
Given $MIP^*$ protocol $V$,
for language $\mathcal{L}$, and
string $x \in \{0,1\}^n$, let
$M_x$ be the TM which
searches for a prover
strategy to convince $V$
to accept $x$ w/ prob
$\geq 1 - s$.
$M_x$ halts $\Leftrightarrow x \in \mathcal{L}$.