Extending Merge Resolution to a Family of QBF-Proof Systems

Sravanthi Chede **Anil Shukla**

Indian Institute of Technology Ropar

Pre-conference workshop FSTTCS
Milestones and Motifs in the Theory of Proofs,
Algebraic Computation, and Lower Bounds
IIT Gandhinagar
December 15, 2024

Quantified Boolean Formulas (QBFs)

- Propositional SAT problem: Given a propositional CNF formula F, determine whether F is satisfiable or not.
- If F is satisfiable, also output a satisfying assignment for it.
- Propositional SAT problem is NP-complete (Cook 1971, Levin 1973).

Quantified Boolean Formulas (QBFs)

- Propositional SAT problem: Given a propositional CNF formula F, determine whether F is satisfiable or not.
- If F is satisfiable, also output a satisfying assignment for it.
- Propositional SAT problem is NP-complete (Cook 1971, Levin 1973).
- QBFs extend propositional logic with Boolean quantifiers $\exists$ and $\forall$.
- $\exists x.F \equiv F|_{x=0} \vee F|_{x=1}$.
- $\forall x.F \equiv F|_{x=0} \wedge F|_{x=1}$.

(QBF warm-up)

- $\phi \equiv (x \vee \neg y) \wedge (\neg x \vee y)$. (Propositional logic)

  ϕ is satisfiable when $x = y$: A satisfying assignment: $x = 0, y = 0$.

(QBF warm-up)

- $\phi \equiv (x \vee \neg y) \wedge (\neg x \vee y)$. (Propositional logic)

  ϕ is satisfiable when $x = y$: A satisfying assignment: $x = 0, y = 0$.
- $\mathcal{F}_1 \equiv \exists x \forall y.(x \vee \neg y) \wedge (\neg x \vee y)$ (QBF)

  Is there exists a value of $x \in \{0, 1\}$ such that for all values of $y \in \{0, 1\}$ $x = y$?

  $\mathcal{F}_1$ is false.

(QBF warm-up)

- $\phi \equiv (x \vee \neg y) \wedge (\neg x \vee y)$. (Propositional logic)

  ϕ is satisfiable when $x = y$: A satisfying assignment: $x = 0, y = 0$.
- $\mathcal{F}_1 \equiv \exists x \forall y.(x \vee \neg y) \wedge (\neg x \vee y)$ (QBF)

  Is there exists a value of $x \in \{0, 1\}$ such that for all values of $y \in \{0, 1\}$ $x = y$?

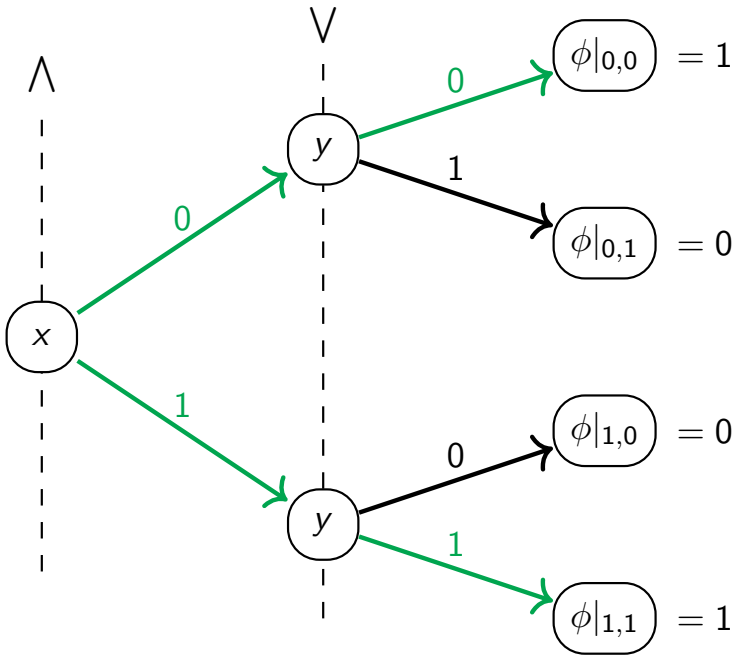
  $\mathcal{F}_1$ is false.
- $\mathcal{F}_2 \equiv \forall x \exists y.(x \vee \neg y) \wedge (\neg x \vee y)$ (QBF)

  Observe, $\mathcal{F}_2$ is true

  For all x, is there exists a y, such that $x = y$?

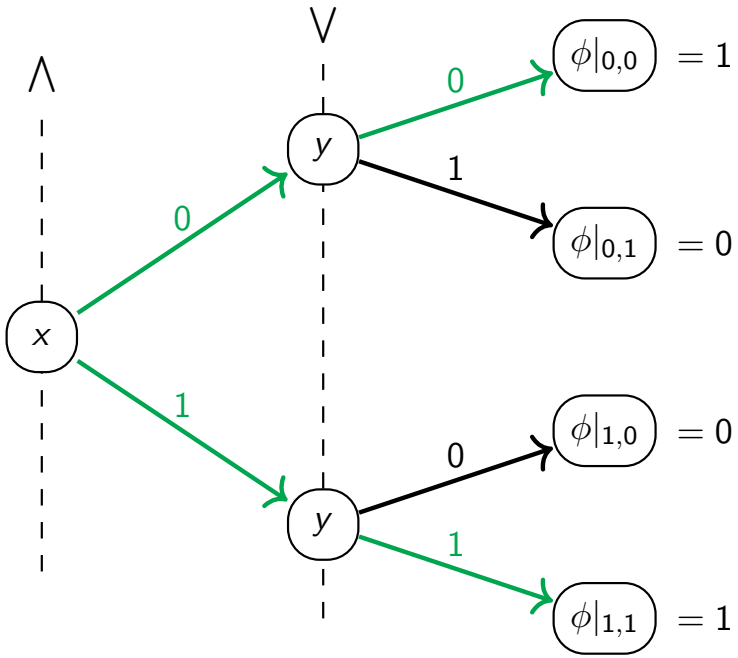
(QBF warm-up)

A model for
$\mathcal{F}_2 \equiv \forall x \exists y.(x \vee \neg y) \wedge (\neg x \vee y)$

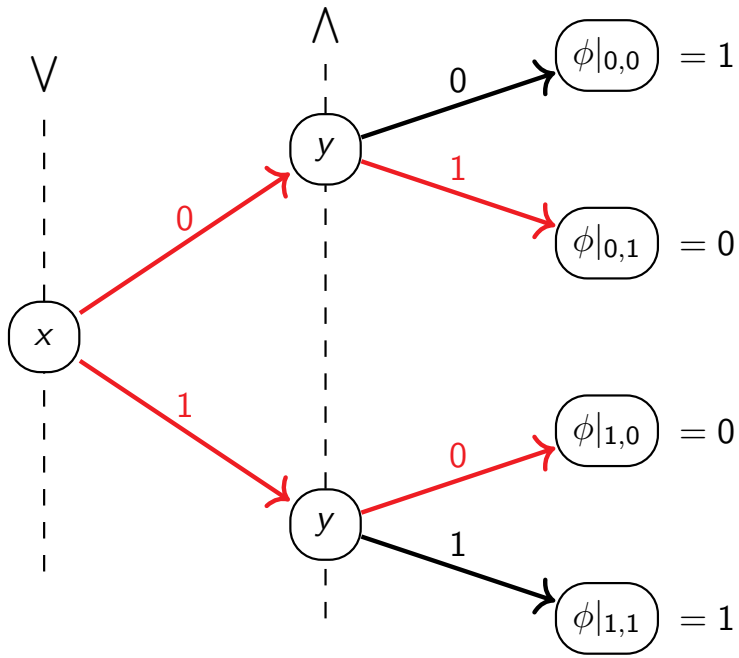


(QBF warm-up)

A model for
$\mathcal{F}_2 \equiv \forall x \exists y.(x \vee \neg y) \wedge (\neg x \vee y)$



A counter-model for
$\mathcal{F}_1 \equiv \exists x \forall y.(x \vee \neg y) \wedge (\neg x \vee y)$



Quantified Boolean Formulas (QBFs)

- $\mathcal{F} = \mathcal{Q}.\phi = \mathcal{Q}_1 X_1 \mathcal{Q}_2 X_2 \ldots \mathcal{Q}_k X_k.\phi(X_1, X_2, \ldots, X_k)$ is a QBF, where
  - $\mathcal{Q}_i \in \{\exists, \forall\}$ and $\mathcal{Q}_i \neq \mathcal{Q}_j$.
  - X_i are pairwise disjoint set of variables.
  - $\phi(X_1, X_2, \ldots X_k)$ is a CNF formula.
  - If $\mathcal{Q}_i = \exists$ (resp.$\mathcal{Q}_i = \forall$), then all variables $x \in X_i$ is called existential (reps. universal) variables.

Quantified Boolean Formulas (QBFs)

- $\mathcal{F} = \mathcal{Q}.\phi = \mathcal{Q}_1 X_1 \mathcal{Q}_2 X_2 \ldots \mathcal{Q}_k X_k.\phi(X_1, X_2, \ldots, X_k)$ is a QBF, where
  - $\mathcal{Q}_i \in \{\exists, \forall\}$ and $\mathcal{Q}_i \neq \mathcal{Q}_j$.
  - X_i are pairwise disjoint set of variables.
  - $\phi(X_1, X_2, \ldots X_k)$ is a CNF formula.
  - If $\mathcal{Q}_i = \exists$ (resp.$\mathcal{Q}_i = \forall$), then all variables $x \in X_i$ is called existential (reps. universal) variables.
  - If a variable $x \in X_i$ and $y \in X_j$, where $i < j$, then we say that x occurs to the left of y in the quantifier prefix (denoted $x \leq_{\mathcal{Q}} y$), and y occurs to the right of x (denoted $y \geq_{\mathcal{Q}} x$).
  - For a universal variable u, let $L_{\mathcal{Q}}(u) = \{x \mid x \text{ is existential and } x \leq_{\mathcal{Q}} u\}$

QBF as a two player game

- A QBF $\mathcal{F} = \mathcal{Q}.\phi = \mathcal{Q}_1 X_1 \mathcal{Q}_2 X_2 \ldots \mathcal{Q}_k X_k.\phi(X_1, X_2, \ldots, X_k)$ can be seen as a game between two players: universal ($\forall$) and existential ($\exists$).
- In the i^{th} step of the game, the player $\mathcal{Q}_i$ assigns values to the variables in X_i.

QBF as a two player game

- A QBF $\mathcal{F} = \mathcal{Q}.\phi = \mathcal{Q}_1 X_1 \mathcal{Q}_2 X_2 \ldots \mathcal{Q}_k X_k.\phi(X_1, X_2, \ldots, X_k)$ can be seen as a game between two players: universal ($\forall$) and existential ($\exists$).
- In the i^{th} step of the game, the player $\mathcal{Q}_i$ assigns values to the variables in X_i.
- The existential player wins if ϕ evaluates to 1 under the assignment constructed in the game.
- The universal player wins if ϕ evaluates to 0.

Winning strategy for QBF

- A strategy for a universal player u is a function from assignments to the variables in $L_{\mathcal{Q}}(u)$ to $\{0, 1\}$.
- A strategy for a universal player is a winning strategy if using this strategy to assign values to universal variables, the $\forall$ player wins any possible game.

Winning strategy for QBF

- A strategy for a universal player u is a function from assignments to the variables in $L_{\mathcal{Q}}(u)$ to $\{0, 1\}$.
- A strategy for a universal player is a winning strategy if using this strategy to assign values to universal variables, the $\forall$ player wins any possible game.
- A QBF is false, if and only if there exists a winning strategy for the universal player.
- Let the language FQBF be the set of all quantified Boolean formulas that are false.
- FQBF is PSPACE-complete [Meyer and Stockmeyer, 1971].

Example of false QBFs

Definition (Beyersdorff, Blinkhorn, Hinde 2019)

Equality (Eq(n)) is the following family of false QBFs:

$$\exists_{i\in[n]} x_i, \forall_{i\in[n]} u_i, \exists_{i\in[n]} t_i.\Big(\bigwedge_{i\in[n]} A_i\Big) \wedge B$$

where

- $B = \exists_{i\in[n]} \overline{t_i}$,
- For $i \in [n]$, A_i contains the following two clauses:

$$(x_i \vee u_i \vee t_i) \quad (\overline{x_i} \vee \overline{u_i} \vee t_i)$$

Example of false QBFs

Definition (Beyersdorff, Blinkhorn, Hinde 2019)

Equality (Eq(n)) is the following family of false QBFs:

$$\exists_{i\in[n]} x_i, \forall_{i\in[n]} u_i, \exists_{i\in[n]} t_i.\Big(\bigwedge_{i\in[n]} A_i\Big) \wedge B$$

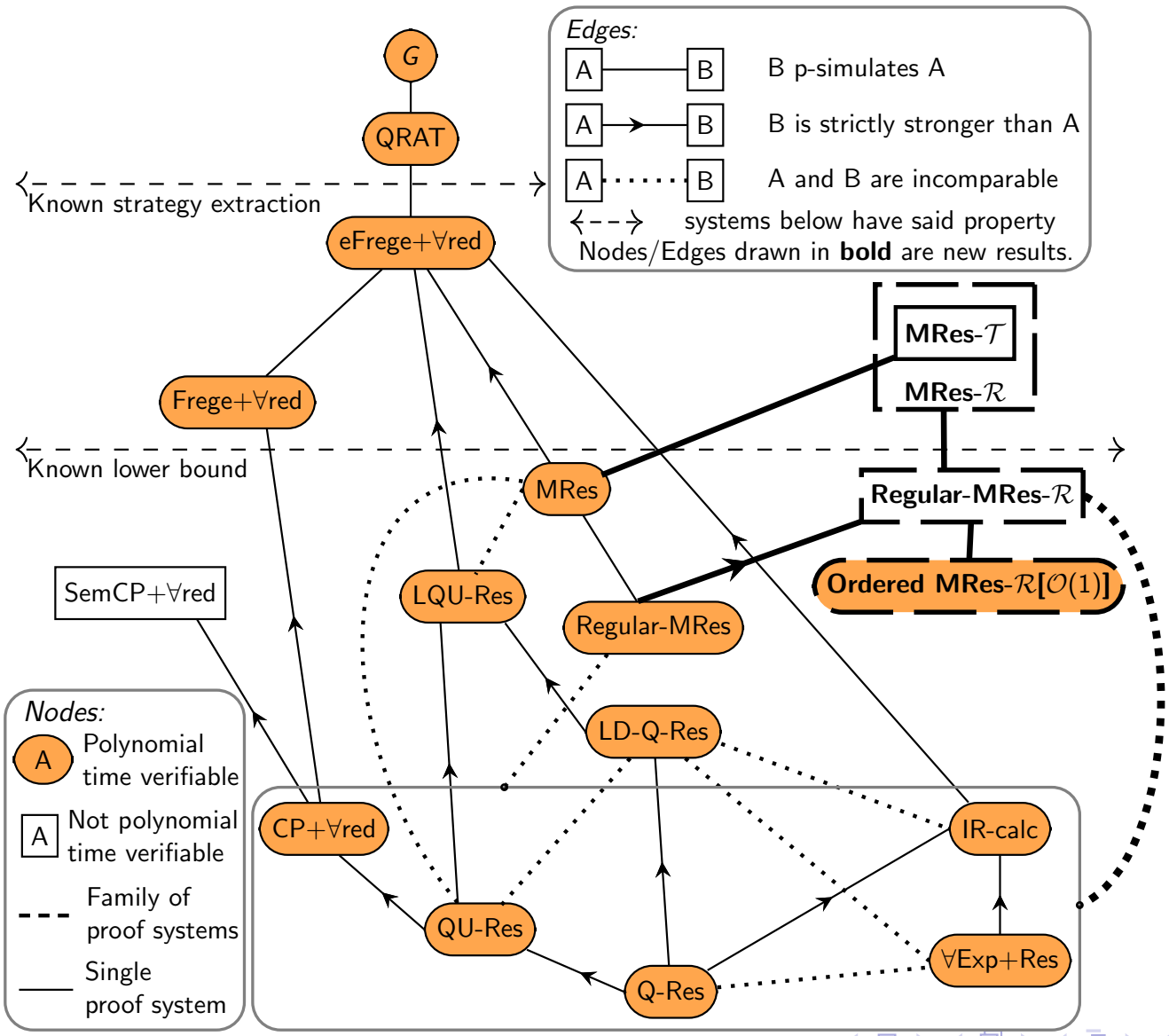
where

- $B = \exists_{i\in[n]} \overline{t_i}$,
- For $i \in [n]$, A_i contains the following two clauses:

$$(x_i \vee u_i \vee t_i) \quad (\overline{x_i} \vee \overline{u_i} \vee t_i)$$

- Eq(n) has a winning strategy of the universal player: For each $i \in [n]$, $u_i = x_i$.

QBFs Proof Systems and their Simulation Hierarchy



Merge (MRes) Resolution (Beyersdorff, Blinkhorn, and Mahajan 2021)

- MRes is a sound and complete proof system for false QBFs.
- That is, for every QBF $\mathcal{F} \in$ FQBF, there exists an MRes proof π, proving the fact that $\mathcal{F} \in$ FQBF. (Completeness)
- If there exists an MRes proof for a QBF $\mathcal{F}$, then $\mathcal{F}$ belongs to FQBF. (Soundness)
- MRes explicitly builds partial winning strategies into its proofs.
- MRes represents the strategies using a variant of binary decision diagrams called merge maps.

MRes-$\mathcal{R}$ proof systems

- Instead of merge maps, can we represent the winning strategies in the proof by some other representations?
- Can we design a general framework of proof systems for false QBFs, where one can use any complete representations for the winning strategies?
- A complete representation is the one in which every possible finite decision function can be represented.

MRes-$\mathcal{R}$ proof systems

- Instead of merge maps, can we represent the winning strategies in the proof by some other representations?
- Can we design a general framework of proof systems for false QBFs, where one can use any complete representations for the winning strategies?
- A complete representation is the one in which every possible finite decision function can be represented.
- We have positive answers to the above questions.
- We introduced a family of proof systems MRes-$\mathcal{R}$, in which winning strategies are stored in any pre-fixed complete representation.

MRes-$\mathcal{R}$ proof systems

- Given false QBF $\mathcal{F} = \mathcal{Q}.\phi$ over existential variables X and universal variables U. An MRes-$\mathcal{R}$ derivation of L_m is a sequence

$$\pi = L_1, L_2, \ldots, L_m \text{ of lines,}$$

where each line $L_i = (C_i, \{H_i^u \ : \ u \in U\})$ is derived using one of the following rules:

  - Axiom rule: There exists a clause $C \in \phi$, and C_i is the existential subclause of C, and for each $u \in U$, H_i^u is the strategy function mapping u to the falsifying u-literal of C.
    Examples:

$$C = (x_1 \vee \overline{u_1} \vee \overline{x_2}) \in \phi \qquad L_i = \Big((x_1 \vee \overline{x_2}), \{H_i^{u_1} = 1, H_i^{u_2} = *\}\Big)$$

$$C = (\overline{x_1} \vee u_2 \vee x_2) \in \phi \qquad L_i = \Big((\overline{x_1} \vee x_2), \{H_i^{u_1} = *, H_i^{u_2} = 0\}\Big)$$

  - Resolution rules:

MRes-$\mathcal{R}$ proof systems

$\pi = L_1, L_2, \ldots, L_m$.

- Resolution rules: Suppose the following lines have been derived:

$$L_a = \Big((C'_a \vee x), \{H^u_a \ : \ u \in U\}\Big); \qquad L_b = \Big((C'_b \vee \overline{x}), \{H^u_b \ : \ u \in U\}\Big)$$

Then L_i is derived as

$\rightarrow \ C_i = (C'_a \vee C'_b)$. Existential variable x is called pivot.

MRes-$\mathcal{R}$ proof systems

$\pi = L_1, L_2, \ldots, L_m$.

- Resolution rules: Suppose the following lines have been derived:

$$L_a = \Big((C'_a \vee x), \{H^u_a \ : \ u \in U\}\Big); \qquad L_b = \Big((C'_b \vee \overline{x}), \{H^u_b \ : \ u \in U\}\Big)$$

Then L_i is derived as

$\rightarrow$ $C_i = (C'_a \vee C'_b)$. Existential variable x is called pivot.

$\rightarrow$ if $x <_{\mathcal{Q}} u$, then $H^u_i = H^u_b \overset{x}{\bowtie} H^u_a$ [if-else branch]

Meaning: if $x = 1$ take H^u_b else take H^u_a

This is same as the **merge** step of MRes

MRes-$\mathcal{R}$ proof systems

$\pi = L_1, L_2, \ldots, L_m$.

- Resolution rules: Suppose the following lines have been derived:

$$L_a = \Big((C'_a \vee x), \{H^u_a \ : \ u \in U\}\Big); \qquad L_b = \Big((C'_b \vee \overline{x}), \{H^u_b \ : \ u \in U\}\Big)$$

Then L_i is derived as

$\rightarrow$ $C_i = (C'_a \vee C'_b)$. Existential variable x is called pivot.

$\rightarrow$ if $x <_{\mathcal{Q}} u$, then $H^u_i = H^u_b \overset{x}{\bowtie} H^u_a$ [if-else branch]

Meaning: if $x = 1$ take H^u_b else take H^u_a

This is same as the **merge** step of MRes

$\rightarrow$ else if $x >_{\mathcal{Q}} u$, then $H^u_i = H^u_a \circ H^u_b$ [consistency + union step]

Here, MRes requires that the non-trivial strategies are isomorphic and picks one of them using the **Select** function.

MRes-$\mathcal{R}$ proof systems

$\pi = L_1, L_2, \ldots, L_m$.

- Resolution rules: Suppose the following lines have been derived:

$$L_a = \Big((C'_a \vee x), \{H^u_a \ : \ u \in U\}\Big); \qquad L_b = \Big((C'_b \vee \overline{x}), \{H^u_b \ : \ u \in U\}\Big)$$

Then L_i is derived as

$\rightarrow$ $C_i = (C'_a \vee C'_b)$. Existential variable x is called pivot.

$\rightarrow$ if $x <_{\mathcal{Q}} u$, then $H^u_i = H^u_b \overset{x}{\bowtie} H^u_a$ [if-else branch]

Meaning: if $x = 1$ take H^u_b else take H^u_a

This is same as the **merge** step of MRes

$\rightarrow$ else if $x >_{\mathcal{Q}} u$, then $H^u_i = H^u_a \circ H^u_b$ [consistency + union step]

Here, MRes requires that the non-trivial strategies are isomorphic and picks one of them using the **Select** function.

π is refuation of $\mathcal{F}$ iff $C_m = \bot$

Operations used in MRes-$\mathcal{R}$ proof systems

Definition (if-else operation (Blinkhorn, Peitl, Slivovsky 2021))

Given two strategies H_1^u and H_2^u and an existential variable x, the if-else operation on these strategies for any complete assignments ε over variables in $L_{\mathcal{Q}}(u)$ gives the strategy H_3^u, denoted as $H_3^u = H_1^u \overset{x}{\bowtie} H_2^u$ as follows:

$$H_3^u(\varepsilon) = \begin{cases} H_1^u(\varepsilon) & : \quad \varepsilon(x) = 1 \\ H_2^u(\varepsilon) & : \quad \varepsilon(x) = 0 \end{cases}$$

Operations used in MRes-$\mathcal{R}$ proof systems

Definition (if-else operation (Blinkhorn, Peitl, Slivovsky 2021))

Given two strategies H_1^u and H_2^u and an existential variable x, the if-else operation on these strategies for any complete assignments ε over variables in $L_{\mathcal{Q}}(u)$ gives the strategy H_3^u, denoted as $H_3^u = H_1^u \overset{x}{\bowtie} H_2^u$ as follows:

$$H_3^u(\varepsilon) = \begin{cases} H_1^u(\varepsilon) & : \quad \varepsilon(x) = 1 \\ H_2^u(\varepsilon) & : \quad \varepsilon(x) = 0 \end{cases}$$

Definition (Blinkhorn, Peitl, Slivovsky 2021)

Let ε and δ be two partial assignments over a set of variables Z. We say that ε and δ are **consistent**, denoted $\varepsilon \simeq \delta$, if for every $x \in Z$ for which $\varepsilon(x) \neq *$ and $\delta(x) \neq *$, we have $\varepsilon(x) = \delta(x)$.

Operations used in MRes-$\mathcal{R}$ proof systems

Definition (if-else operation (Blinkhorn, Peitl, Slivovsky 2021))

Given two strategies H_1^u and H_2^u and an existential variable x, the if-else operation on these strategies for any complete assignments ε over variables in $L_{\mathcal{Q}}(u)$ gives the strategy H_3^u, denoted as $H_3^u = H_1^u \overset{x}{\bowtie} H_2^u$ as follows:

$$H_3^u(\varepsilon) = \begin{cases} H_1^u(\varepsilon) & : \quad \varepsilon(x) = 1 \\ H_2^u(\varepsilon) & : \quad \varepsilon(x) = 0 \end{cases}$$

Definition (Blinkhorn, Peitl, Slivovsky 2021)

Let ε and δ be two partial assignments over a set of variables Z. We say that ε and δ are **consistent**, denoted $\varepsilon \simeq \delta$, if for every $x \in Z$ for which $\varepsilon(x) \neq *$ and $\delta(x) \neq *$, we have $\varepsilon(x) = \delta(x)$.

Example: $Z = \{x_1, x_2, x_3\}$, $\varepsilon : x_1 = 0, x_2 = *, x_3 = 1$, $\delta : x_1 = *, x_2 = 1, x_3 = 1$. Then $\varepsilon \simeq \delta$.

Operations used in MRes-$\mathcal{R}$ proof systems

Definition (Blinkhorn, Peitl, Slivovsky 2021)

Two strategies H_1^u and H_2^u for a universal player u are **consistent** (denoted $H_1^u \simeq H_2^u$), if the u-assignments given by $H_1^u(\varepsilon)$ and $H_2^u(\varepsilon)$ are consistent for every possible $L_{\mathcal{Q}}(u)$ assignments.

- Treat (partial) assignments as a set of literals it satisfies.
- That is, let ε is a partial assignment over variables X. Then ε can be view as a set $\{x \mid \varepsilon(x) = 1\} \cup \{\overline{x} \ : \ \varepsilon(x) = 0\}$.

Operations used in MRes-$\mathcal{R}$ proof systems

Definition (Blinkhorn, Peitl, Slivovsky 2021)

Two strategies H_1^u and H_2^u for a universal player u are **consistent** (denoted $H_1^u \simeq H_2^u$), if the u-assignments given by $H_1^u(\varepsilon)$ and $H_2^u(\varepsilon)$ are consistent for every possible $L_{\mathcal{Q}}(u)$ assignments.

- Treat (partial) assignments as a set of literals it satisfies.
- That is, let ε is a partial assignment over variables X. Then ε can be view as a set $\{x \mid \varepsilon(x) = 1\} \cup \{\overline{x} \ : \ \varepsilon(x) = 0\}$.
- If two (partial) assignments ε and δ are consistent, the union of ε and δ (denoted $\varepsilon \circ \delta$) is just the union of their corresponding sets.
- Since consistency checks are hard in general, the proof systems in MRes-$\mathcal{R}$ are not polynomial-time verifiable.

Soundness and Completeness of MRes-$\mathcal{R}$

Lemma (Soundness)

Let $(\emptyset, \{H^u : u \in U\})$ be a last line in an MRes-$\mathcal{R}$ refutation of a QBF $\mathcal{F}$. Then the function computed by $\{H^u : u \in U\}$ form a countermodel for $\mathcal{F}$.

We show completeness of MRes-$\mathcal{R}$ in two steps:

Lemma

MRes-$\mathcal{M}$ (that is, MRes-$\mathcal{R}$ using merge maps as representations) p-simulates MRes.

Since MRes is complete, MRes-$\mathcal{M}$ is also complete via the above Lemma.

Soundness and Completeness of MRes-$\mathcal{R}$

Lemma (Soundness)

Let $(\emptyset, \{H^u : u \in U\})$ be a last line in an MRes-$\mathcal{R}$ refutation of a QBF $\mathcal{F}$. Then the function computed by $\{H^u : u \in U\}$ form a countermodel for $\mathcal{F}$.

We show completeness of MRes-$\mathcal{R}$ in two steps:

Lemma

MRes-$\mathcal{M}$ (that is, MRes-$\mathcal{R}$ using merge maps as representations) p-simulates MRes.

Since MRes is complete, MRes-$\mathcal{M}$ is also complete via the above Lemma.

Lemma

Every MRes-$\mathcal{M}$ proof can be transformed into an MRes-$\mathcal{R}$ proof for any complete representation R in exponential time.

Regular MRes-$\mathcal{R}$ is exponentially stronger than regular MRes

- Any MRes-$\mathcal{R}$ proof π can be viewed as a directed acyclic graph G_π where edges goes from hypothesis to the conclusions.
- Let S be a subset of existential variables X of a QBF $\mathcal{F}$.
- An MRes-$\mathcal{R}$ proof π is called S-regular if for every $x \in S$, there is no leaf-to-root path in G_π that uses x more than once as a pivot.
- An X-regular MRes-$\mathcal{R}$ refutation is simply a regular refutation.

Regular MRes-$\mathcal{R}$ is exponentially stronger than regular MRes

- Any MRes-$\mathcal{R}$ proof π can be viewed as a directed acyclic graph G_π where edges goes from hypothesis to the conclusions.
- Let S be a subset of existential variables X of a QBF $\mathcal{F}$.
- An MRes-$\mathcal{R}$ proof π is called S-regular if for every $x \in S$, there is no leaf-to-root path in G_π that uses x more than once as a pivot.
- An X-regular MRes-$\mathcal{R}$ refutation is simply a regular refutation.
- There exists a family of false QBFs $\mathcal{H}$-Eq$^2(n)(R_0, R_1)$ (Squared-Equality-with-Holes) which are hard to refute for regular MRes but are easy to refute in regular MRes-$\mathcal{R}$.
- $\mathcal{H}$-Eq$^2(n)(R_0, R_1)$ is a variant of Eq$^2(n)$.

Regular MRes-$\mathcal{R}$ is exponentially stronger than regular MRes

Definition ($\mathrm{Eq}^2(n)$ (Beyersdorff, Blinkhorn, Mahajan 2021))

$$\underset{i\in[n]}{\exists} x_i, \underset{j\in[n]}{\exists} y_j \underset{i\in[n]}{\forall} u_i, \underset{j\in[n]}{\forall} v_j \underset{i,j\in[n]}{\exists} t_{i,j}.\left(\underset{i,j\in[n]}{\wedge} A_{i,j}\right) \wedge B$$

- $B = \underset{i,j\in[n]}{\vee} \overline{t_{i,j}}$
- For $i, j \in [n]$, $A_{i,j}$ contains the following four clauses:

$$x_i \vee y_j \vee u_i \vee v_j \vee t_{i,j} \qquad x_i \vee \overline{y_j} \vee u_i \vee \overline{v_j} \vee t_{i,j}$$
$$\overline{x_i} \vee y_j \vee \overline{u_i} \vee v_j \vee t_{i,j} \qquad \overline{x_i} \vee \overline{y_j} \vee \overline{u_i} \vee \overline{v_j} \vee t_{i,j}$$

- Winning strategy: for all $i \in [n]$, set $u_i = x_i$; and for all $j \in [n]$, set $v_j = y_j$.
- $\mathrm{Eq}^2(n)$ is easy for regular MRes.

Regular MRes-$\mathcal{R}$ is exponentially stronger than regular MRes

- From the clauses $A_{i,j}$'s of $\mathrm{Eq}^2(n)$, the universal variables are removed carefully in such a way that the resulting QBF is still false but becomes hard for regular MRes.

Regular MRes-$\mathcal{R}$ is exponentially stronger than regular MRes

- From the clauses $A_{i,j}$'s of $\mathrm{Eq}^2(n)$, the universal variables are removed carefully in such a way that the resulting QBF is still false but becomes hard for regular MRes.
- $\mathcal{H}$-$\mathrm{Eq}^2(n)(R_0, R_1)$ identifies two regions in the $[n] \times [n]$ grid and changes the $A_{i,j}$ clauses of $\mathrm{Eq}^2(n)$ based on the regions (i, j) belongs to.
- $\mathcal{H}$-$\mathrm{Eq}^2(n)(R_0, R_1)$ can use any partition of $[n] \times [n]$ grid into two regions R_0, R_1 such that each region has at least one position in each row and at least one position in each column.
- We call such partition R_0, R_1 as covering partition.

Regular MRes-$\mathcal{R}$ is exponentially stronger than regular MRes

- From the clauses $A_{i,j}$'s of $\text{Eq}^2(n)$, the universal variables are removed carefully in such a way that the resulting QBF is still false but becomes hard for regular MRes.
- $\mathcal{H}$-$\text{Eq}^2(n)(R_0, R_1)$ identifies two regions in the $[n] \times [n]$ grid and changes the $A_{i,j}$ clauses of $\text{Eq}^2(n)$ based on the regions (i, j) belongs to.
- $\mathcal{H}$-$\text{Eq}^2(n)(R_0, R_1)$ can use any partition of $[n] \times [n]$ grid into two regions R_0, R_1 such that each region has at least one position in each row and at least one position in each column.
- We call such partition R_0, R_1 as covering partition.

Lemma (Mahajan and Sood 2022)

$\mathcal{H}$-$Eq^2(n)(R_0, R_1)$ requires exponential-size refutations in regular MRes

$\mathcal{H}$-Eq$^2(n)(R_0, R_1)$

Definition (Mahajan and Sood 2022)

$$\underset{i\in[n]}{\exists} x_i, \underset{j\in[n]}{\exists} y_j \underset{i\in[n]}{\forall} u_i, \underset{j\in[n]}{\forall} v_j \underset{i,j\in[n]}{\exists} t_{i,j}.\left(\underset{i,j\in[n]}{\wedge} A_{i,j}\right) \wedge B$$

- $B = \underset{i,j\in[n]}{\vee} \overline{t_{i,j}}$
- For $(i,j) \in R_0$, $A_{i,j}$ contains the following four clauses:

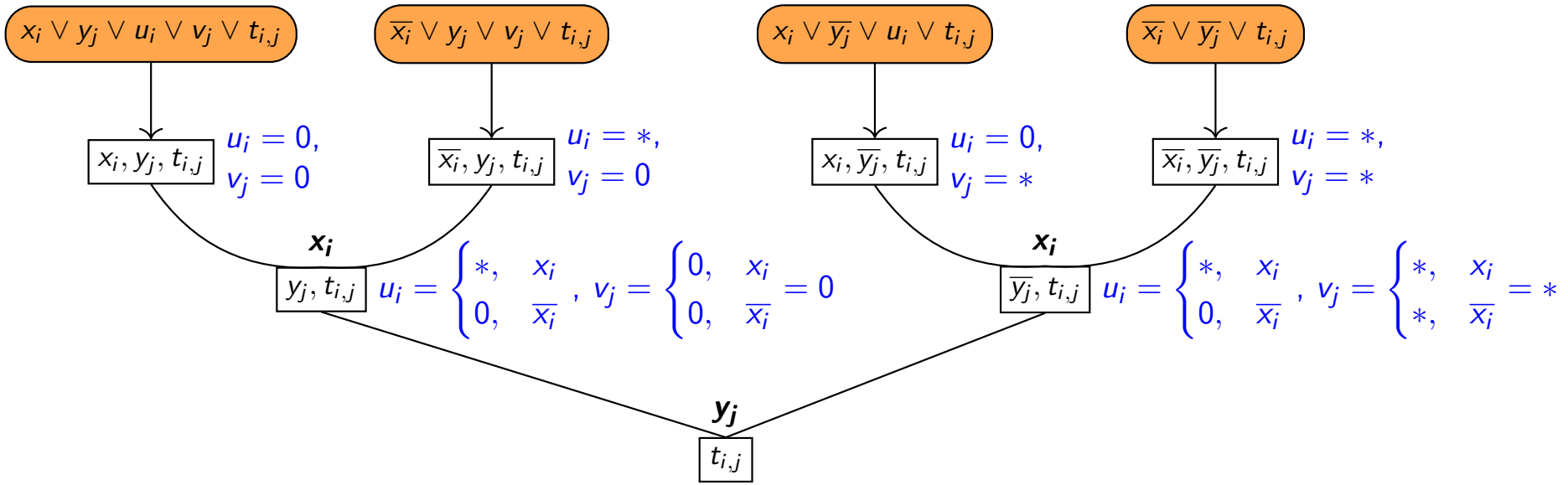
$$x_i \vee y_j \vee u_i \vee v_j \vee t_{i,j} \qquad x_i \vee \overline{y_j} \vee u_i \vee t_{i,j}$$
$$\overline{x_i} \vee y_j \vee v_j \vee t_{i,j} \qquad \overline{x_i} \vee \overline{y_j} \vee t_{i,j}$$

- For $(i,j) \in R_1$, $A_{i,j}$ contains the following four clauses:

$$x_i \vee y_j \vee t_{i,j} \qquad x_i \vee \overline{y_j} \vee \overline{v_j} \vee t_{i,j}$$
$$\overline{x_i} \vee y_j \vee \overline{u_i} \vee t_{i,j} \qquad \overline{x_i} \vee \overline{y_j} \vee \overline{u_i} \vee \overline{v_j} \vee t_{i,j}$$

Linear size refutation of $\mathcal{H}$-Eq$^2(n)(R_0, R_1)$ in regular MRes-$\mathcal{R}$

For $(i,j) \in R_0$: $\underset{i\in[n]}{\exists} x_i, \underset{j\in[n]}{\exists} y_j \underset{i\in[n]}{\forall} u_i, \underset{j\in[n]}{\forall} v_j \underset{i,j\in[n]}{\exists} t_{i,j}$

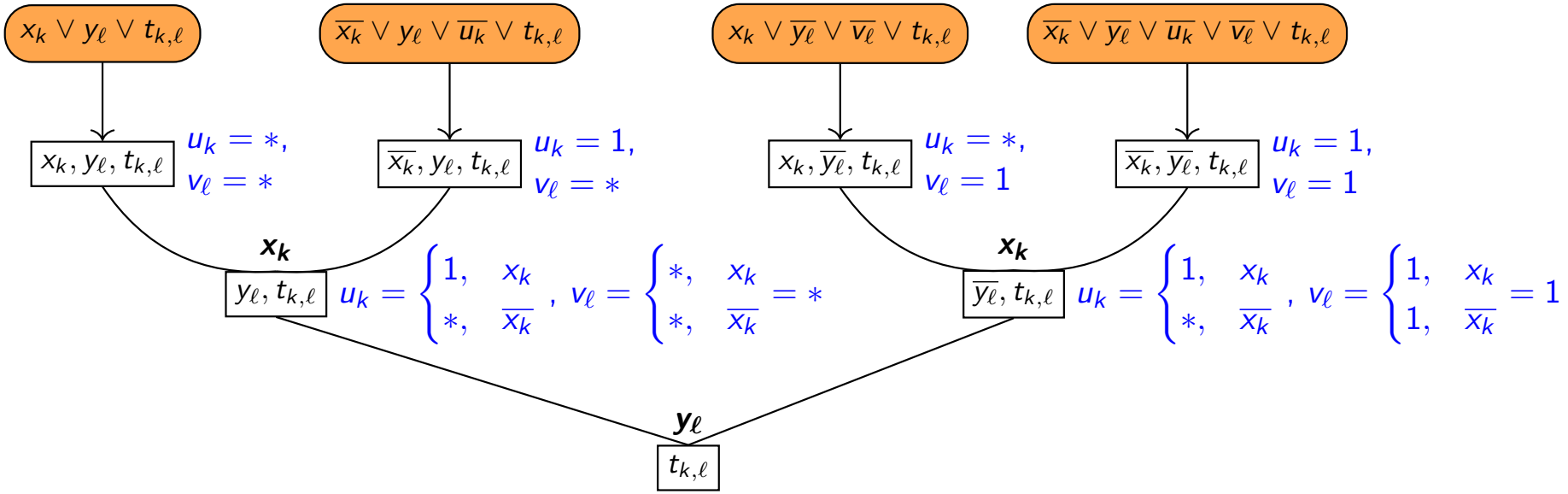


$$u_i = \begin{cases} *, & x_i y_j \\ *, & x_i \overline{y_j} \\ 0, & \overline{x_i} y_j \\ 0, & \overline{x_i y_j} \end{cases} = \begin{cases} *, & x_i \\ 0, & \overline{x_i} \end{cases}, \; v_j = \begin{cases} *, & y_j \\ 0, & \overline{y_j} \end{cases}$$

Linear size refutation of $\mathcal{H}$-Eq$^2(n)(R_0, R_1)$ in regular MRes-$\mathcal{R}$ (Contd.)

For $(k, \ell) \in R_1$:

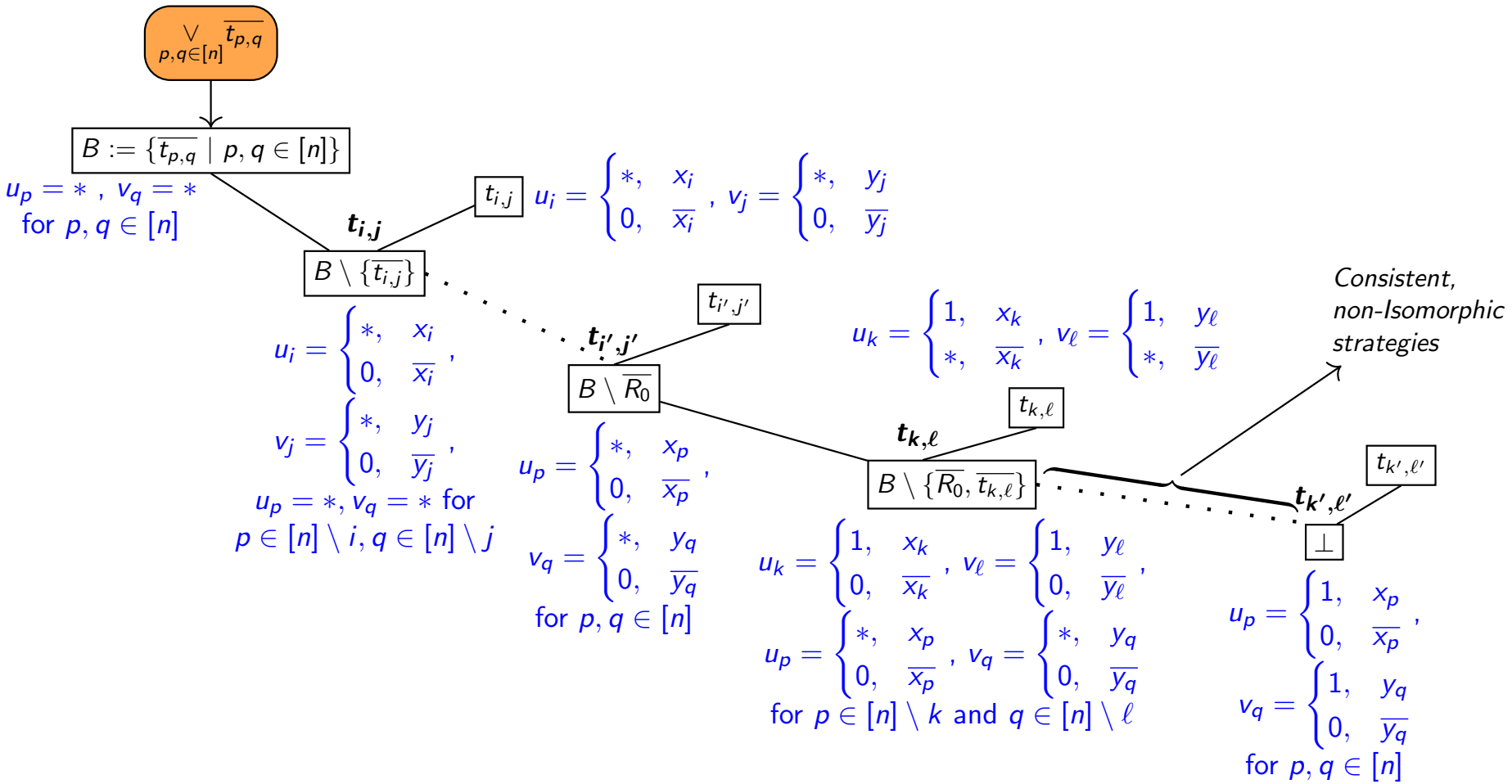
$$\exists_{i \in [n]} x_i, \exists_{j \in [n]} y_j \forall_{i \in [n]} u_i, \forall_{j \in [n]} v_j \exists_{i,j \in [n]} t_{i,j}$$



$$u_k = \begin{cases} 1, & x_k y_\ell \\ 1, & x_k \overline{y_\ell} \\ *, & \overline{x_k} y_\ell \\ *, & \overline{x_k y_\ell} \end{cases} = \begin{cases} 1, & x_k \\ *, & \overline{x_k} \end{cases}, v_\ell = \begin{cases} 1, & y_\ell \\ *, & \overline{y_\ell} \end{cases}$$

Linear size refutation of $\mathcal{H}$-Eq$^2(n)(R_0, R_1)$ in regular MRes-$\mathcal{R}$ (Contd.)

$(i,j),\ldots,(i',j') \in R_0$, $(k,\ell),\ldots,(k',\ell') \in R_1$: $\exists_{i\in[n]} x_i, \exists_{j\in[n]} y_j \forall_{i\in[n]} u_i, \forall_{j\in[n]} v_j \exists_{i,j\in[n]} t_{i,j}$



Lower bounds for regular MRes-$\mathcal{R}$

- Beyersdorff et al., 2020 showed that the Completion Principle Formulas CR_n (Janota and Marques-Silva 2015) are hard for regular MRes.
- We lift the lower bound proof of CR_n to regular MRes-$\mathcal{R}$ as well.

Lower bounds for regular MRes-$\mathcal{R}$

- Beyersdorff et al., 2020 showed that the Completion Principle Formulas CR_n (Janota and Marques-Silva 2015) are hard for regular MRes.
- We lift the lower bound proof of CR_n to regular MRes-$\mathcal{R}$ as well.

The Completion Principle: Consider two sets $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$, and depict their cross product $A \times B$ as in the table below.

a_1	a_1	$\ldots$	a_1	a_2	a_2	$\ldots$	a_2	$\ldots$	$\ldots$	a_n	a_n	$\ldots$	a_n
b_1	b_2	$\ldots$	b_n	b_1	b_2	$\ldots$	b_n	$\ldots$	$\ldots$	b_1	b_2	$\ldots$	b_n

The Completion Principle

a_1	a_1	$\ldots$	a_1	a_2	a_2	$\ldots$	a_2	$\ldots$	$\ldots$	a_n	a_n	$\ldots$	a_n
b_1	b_2	$\ldots$	b_n	b_1	b_2	$\ldots$	b_n	$\ldots$	$\ldots$	b_1	b_2	$\ldots$	b_n

- The following two player game is played on the above table:
- In the first round, player 1 deletes exactly one cell from each column.
- In the second round, player 2 chooses one of the two rows.
- Player 2 wins if the chosen row contains either the complete set A or the set B; otherwise player 1 wins.
- It is well known that player 2 has a winning strategy:

The Completion Principle: Player 2 winning strategy

a_1	a_1	$\ldots$	a_1	a_2	a_2	$\ldots$	a_2	$\ldots$	$\ldots$	a_n	a_n	$\ldots$	a_n
b_1	b_2	$\ldots$	b_n	b_1	b_2	$\ldots$	b_n	$\ldots$	$\ldots$	b_1	b_2	$\ldots$	b_n

Winning strategy of player 2:

- Suppose, after player 1 plays, some a_i is missing in the top row. Then the entire set B below the a_i chunk is present in the bottom row and so player 2 chooses the bottom row to win.
- Otherwise, no a_i is missing in the top row, so player 2 can win by choosing the top row.
- This fact (that player 2 can always win) is called the completion principle.

The false QBF CR_n

- CR_n encodes that player 1 has a winning strategy.
- For each (i, j) column of the table $\begin{bmatrix} a_i \\ b_j \end{bmatrix}$, we have a variable $x_{i,j}$.
- Let $x_{i,j} = 0$ denote that player 1 keeps a_i (i.e., deletes b_j) from $(i, j)^{\text{th}}$ column.
- $x_{i,j} = 1 \implies$ player 1 keeps b_j.

The false QBF CR_n

- CR_n encodes that player 1 has a winning strategy.
- For each (i, j) column of the table $\begin{bmatrix} a_i \\ b_j \end{bmatrix}$, we have a variable $x_{i,j}$.
- Let $x_{i,j} = 0$ denote that player 1 keeps a_i (i.e., deletes b_j) from $(i, j)^{\text{th}}$ column.
- $x_{i,j} = 1 \implies$ player 1 keeps b_j.
- Let the variable z denote the choice of player 2: $z = 0 \implies$ player 2 chooses the top row.
- For $i, j \in [n]$, Boolean variables a_i, b_j encode that for the chosen values of all the $x_{k,\ell}$, and the row chosen via z, at least one copy of the element a_i and b_j, respectively, is kept.
- For example: $(x_{i,j} \wedge z) \Rightarrow b_j$.

The false QBF CR_n

Definition (CR_n (Janota and Marques-Silva 2015))

$$\exists_{i,j\in[n]} x_{i,j}, \forall z, \exists_{i\in[n]} a_i, \exists_{j\in[n]} b_j . \Big(\bigwedge_{i,j\in[n]} (A_{i,j} \wedge B_{i,j}) \Big) \wedge L_A \wedge L_B, \text{ where}$$

- $A_{i,j} = x_{i,j} \vee z \vee a_i$
- $B_{i,j} = \overline{x_{i,j}} \vee \overline{z} \vee b_j$
- $L_A = \overline{a_1} \vee \overline{a_2} \vee \cdots \vee \overline{a_n}$
- $L_B = \overline{b_1} \vee \overline{b_2} \vee \cdots \vee \overline{b_n}$

Theorem

Every regular MRes-$\mathcal{R}$ refutation of CR_n has size $2^{\Omega(n)}$

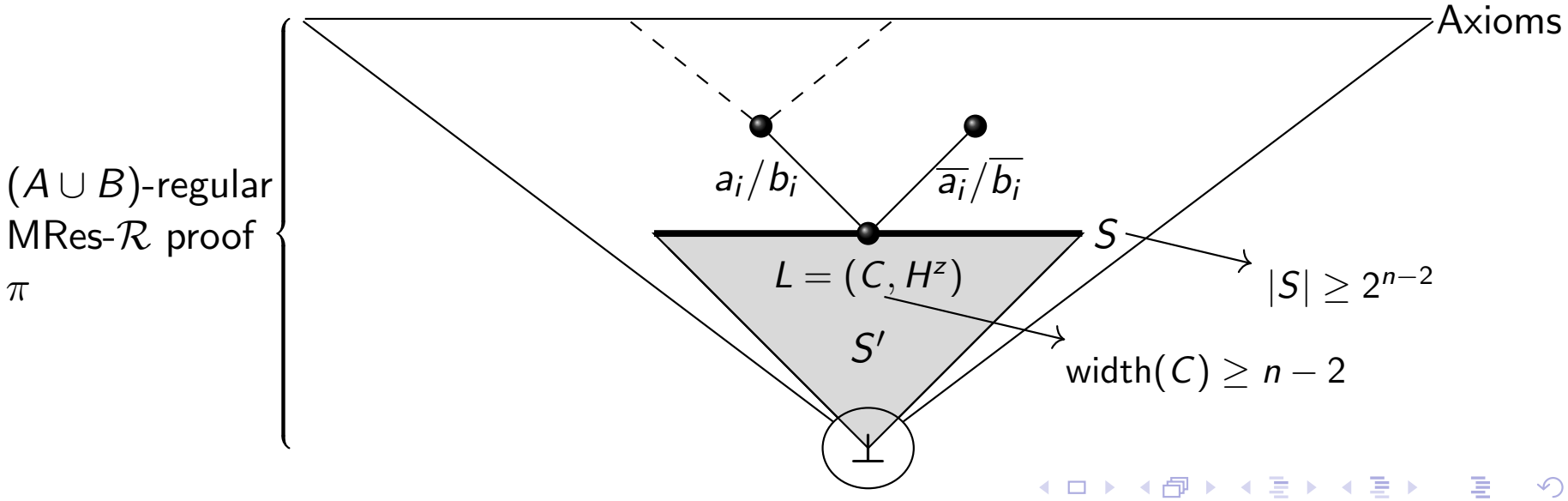
Lower bound for regular MRes-$\mathcal{R}$

Theorem

Every $(A \cup B)$-regular MRes-$\mathcal{R}$ refutation of CR_n has size $2^{\Omega(n)}$

Proof outline: Let π be any $(a \cup B)$-regular MRes-$\mathcal{R}$ proof.

- S' : All lines $L = (C, H)$ where C has no variables from $A \cup B$ and there exists a path from L to $\bot$ with only clauses from S'. $\bot \in S'$
- S : Boundary of S'. That is, all lines $\in S'$ whose hypothesis are $\notin S'$.



Lower bound for regular MRes-$\mathcal{R}$ (Contd.)

- Let $F = \bigwedge_{(C,H^u)\in S} C$.
- F is a false CNF formula over n^2 variables $X = \{x_{i,j} \ : \ i,j \in [n]\}$.
- For a clause C, let width(C) is equal to the number of literals in C.

Lemma

For all $C \in F$, width$(C) \geq n-2$. That is, for all $L = (C, H^u) \in S$, width$(C) \geq n-2$.

- Each clause C can only be falsified by an assignment by setting at least $n-2$ literals to zero.

Lower bound for regular MRes-$\mathcal{R}$ (Contd.)

- For any $C \in F$, the number of assignments which falsifies C is at most $2^{n^2-(n-2)}$.
- Since, F is unsatisfiable, every assignment to X must falsify at least one clause $\in F$.
- There are total 2^{n^2} assignments to X.
- Therefore, the number of clauses in F is at least $\frac{2^{n^2}}{2^{n^2-(n-2)}} = 2^{(n-2)}$.
- Therefore, the number of lines in π is at least 2^{n-2}.

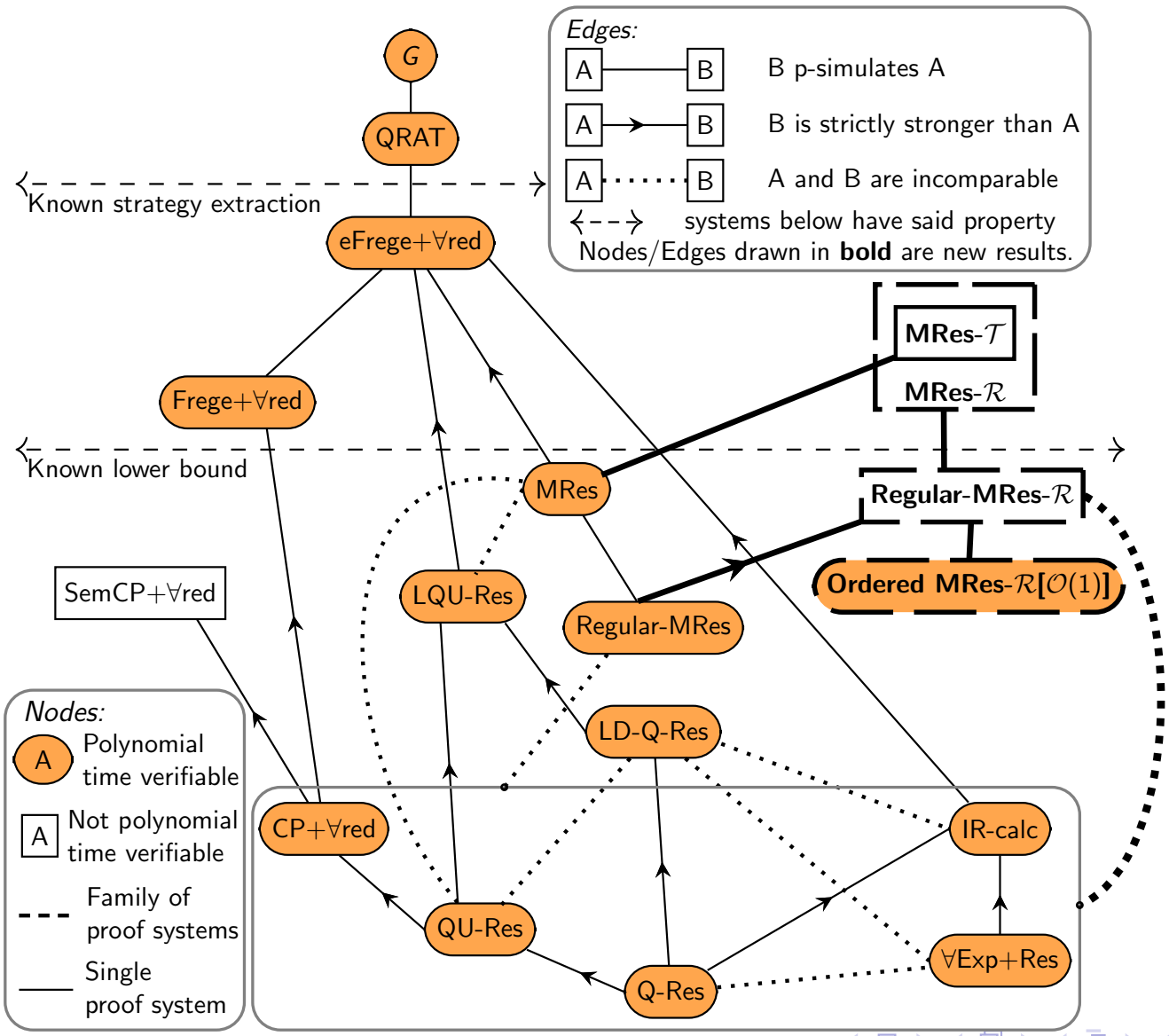
Ordered MRes-$\mathcal{R}$ with OBDD representation is polynomial-time verifiable

- Since consistency checking is hard in general, MRes-$\mathcal{R}$ proof systems is not polynomial-time verifiable in general.
- An MRes-$\mathcal{R}$ proof systems, which uses a complete representation in which consistency checking, union, and if-else operations are efficient is polynomial-time verifiable.
- One such representation is the OBDDs (Ordered Binary Decision Diagrams) with a fixed ordering of variables.

Lemma

Ordered MRes-$\mathcal{R}$ with OBDD representation is polynomial-time verifiable.

QBFs Proof Systems and their Simulation Hierarchy



Open problems

1. Are there exists a family of QBFs which are easy to refute in MRes-$\mathcal{R}$ but are hard for MRes?
2. Does there exist a family of false QBFs which are hard to refute in MRes-$\mathcal{R}$.

Thank you.