Merge Resolution: QBF proofs with inbuilt strategies

Meena Mahajan

The Institute of Mathematical Sciences,
Homi Bhabha National Institute,
Chennai, India.

04 July 2022

(Mathematical Approaches to Lower Bounds:
Complexity of Proofs and Computation)

(ICMS, Edinburgh. 04-08 July 2022)

Merge Resolution: QBF proofs with inbuilt strategies

Joint work Olaf Beyersdorff,
Joshua Blinkhorn,
Tomáš Peitl, and
Gaurav Sood.

Results reported in

- STACS 2019 / Journal of Automated Reasoning 2021,
- FSTTCS 2020 / ECCC TR 2020-188,
- SAT 2022.

Propositional Satisfiability

- SAT: Satisfiability.
  eg. Is there an assignment to x, y, z satisfying all the clauses
  $(x \vee y \vee z), (x \vee \neg y \vee \neg z), (\neg x \vee y \vee \neg z), (\neg x \vee \neg y \vee z)$?
- Quintessential NP-complete problem.
- Very hard – in theory.

  In practice – a solved problem! Many good SAT solvers around.

Propositional Satisfiability

- SAT: Satisfiability.
  eg. Is there an assignment to x, y, z satisfying all the clauses
  $(x \vee y \vee z), (x \vee \neg y \vee \neg z), (\neg x \vee y \vee \neg z), (\neg x \vee \neg y \vee z)$?
- Quintessential NP-complete problem.
- Very hard – in theory.

  In practice – a solved problem! Many good SAT solvers around.
- Ambitious ongoing programs to design good solvers for problems harder than SAT.
- Focus of this talk: QBF.

QBF: Quantified Boolean Formulas

- We consider QBFs that are
  - totally quantified (no unbound variables),
  - in prenex form,
  - with inner propositional formula in CNF.
- e.g. Is this formula true?

$$\exists e\ \forall u\ \exists c\ \exists d \quad (\neg e \vee c)(e \vee d)(\neg u \vee c)(u \vee d)(\neg c \vee \neg d)$$

QBF: Quantified Boolean Formulas

- We consider QBFs that are
  - totally quantified (no unbound variables),
  - in prenex form,
  - with inner propositional formula in CNF.
- e.g. Is this formula true?

$$\exists e\ \forall u\ \exists c\ \exists d \quad (\neg e \vee c)(e \vee d)(\neg u \vee c)(u \vee d)(\neg c \vee \neg d)$$

- QBF subsumes SAT. eg. Is this QBF true?

$$\exists x \exists y \exists z (x \vee y \vee z) \wedge (x \vee \neg y \vee \neg z) \wedge (\neg x \vee y \vee \neg z) \wedge (\neg x \vee \neg y \vee z)$$

QBF: Quantified Boolean Formulas

- We consider QBFs that are
  - totally quantified (no unbound variables),
  - in prenex form,
  - with inner propositional formula in CNF.
- e.g. Is this formula true?

$$\exists e \; \forall u \; \exists c \; \exists d \quad (\neg e \vee c)(e \vee d)(\neg u \vee c)(u \vee d)(\neg c \vee \neg d)$$

- QBF subsumes SAT. eg. Is this QBF true?

$$\exists x \exists y \exists z (x \vee y \vee z) \wedge (x \vee \neg y \vee \neg z) \wedge (\neg x \vee y \vee \neg z) \wedge (\neg x \vee \neg y \vee z)$$

- QBF more succinctly expressive than SAT; PSPACE-complete.

QBF Proof Complexity

- Quite a few QBF solvers developed in the last couple of decades.
- Underlying solver heuristics are formal proof systems: Runs of SAT/QBF solver on false QBFs provide proofs of unsatisfiability/falsity.
- Lower bounds in formal proof system
  (no short proof of unsat/falsity)
  $\Downarrow$
  no short runs.
- Proving lower bounds – proof complexity

The two-player evaluation game

- QBF $Q\vec{x} \cdot F(x)$
- Two players, $P_\exists$ and $P_\forall$, step through quantifier prefix left-to-right. $P_\exists$ picks values for $\exists$ variables, $P_\forall$ for $\forall$ variables.

  Assignment constructed on a run: $\tilde{a}$.

  $P_\exists$ wins a run of the game if $F(\tilde{a})$ true. Otherwise $P_\forall$ wins.
- $Q\vec{x} \cdot F(x)$ true if and only if $P_\exists$ has a winning strategy.
- $Q\vec{x} \cdot F(x)$ false if and only if $P_\forall$ has a winning strategy.

How to prove that a false QBF is false

- Start with initial set of clauses.
- Derive and add clauses to set until falseness is obvious.

How to prove that a false QBF is false

- Start with initial set of clauses.
- Derive and add clauses to set until falseness is obvious.

- To achieve soundness:
  - Preserve $P_\exists$ winning strategies.
  - Finally derive empty clause $\Box$.
    (This defeats every potential $P_\exists$ strategy.)
- To achieve completeness:
  - From a $P_\forall$ winning strategy, use rules to derive $\Box$.

An example QBF Proof System

- e.g. Two rules that preserve $P_\exists$ winning strategies:

* Resolution: $\dfrac{x \vee A \qquad \overline{x} \vee B}{A \vee B}$

* Universal reduction:
$\dfrac{A \vee u}{A}$ $(\mathrm{var}(u)$ is universal, and right of all variables in $A)$

An example QBF Proof System

- e.g. Two rules that preserve $P_\exists$ winning strategies:

* Resolution: $\dfrac{x \vee A \qquad \overline{x} \vee B}{A \vee B}$

* Universal reduction:
$\dfrac{A \vee u}{A}$ ($\mathrm{var}(u)$ is universal, and right of all variables in A)

- The QURes proof system (a.k.a. Res+$\forall$Red):
Resolution + Universal Reduction.

More sophisticated rules

- Creating tautologies can be unsound.
  Refutation of True QBF? $\forall u \exists x (x \vee u)(\neg x \vee \neg u)$.

$$\dfrac{\dfrac{\dfrac{x \vee u \qquad \neg x \vee \neg u}{u \vee \neg u}}{u}}{\Box}$$

More sophisticated rules

- Creating tautologies can be unsound.
  Refutation of True QBF? $\forall u \exists x (x \vee u)(\neg x \vee \neg u)$.

$$\begin{array}{c} x \vee u \qquad \neg x \vee \neg u \\ \hline u \vee \neg u \\ \hline u \\ \hline \square \end{array}$$

- Creating seeming tautologies can be meaningful and sound.
  $\exists x \forall u (x \vee u)(\neg x \vee \neg u)$

$$\begin{array}{c} x \vee u \qquad \neg x \vee \neg u \\ \hline u^{*} \\ \hline \square \end{array}$$

More sophisticated rules

- Creating tautologies can be unsound.
  Refutation of True QBF? $\forall u \exists x (x \vee u)(\neg x \vee \neg u)$.

$$\dfrac{\dfrac{\dfrac{x \vee u \qquad \neg x \vee \neg u}{u \vee \neg u}}{u}}{\square}$$

- Creating seeming tautologies can be meaningful and sound.
  $\exists x \forall u (x \vee u)(\neg x \vee \neg u)$

$$\dfrac{\dfrac{x \vee u \qquad \neg x \vee \neg u}{u^*}}{\square}$$

- Long-Distance QResolution LDQRes,and generalisations $\mathrm{LQU}^+\mathrm{Res}$:
  - Allow u and $\neg u$ to be combined into u^*, provided u right of pivot.
  - Disallow resolution with pivot x if $u < x$ and antecedents contain "conflicting" $u, \neg u, u^*$.

Proving Soundness

- In Res+$\forall$Red, preserving $P_\exists$ winning strategies $\implies$ soundness.
  In more sophisticated systems?
- Strategy extraction:
  From refutation, extract a $P_\forall$ winning strategy.
- Already quite complex for LDQRes.
  To keep it manageable, LDQRes syntax also blocks some seemingly sound steps.

A new QBF proof system: MRes

- The key idea: Preserve and Augment partial $P_\forall$ winning strategies.

  Construct partial strategies for $P_\forall$ explicitly,
  building up to a winning strategy.

A new QBF proof system: MRes

- The key idea: Preserve and Augment partial $P_\forall$ winning strategies.
  Construct partial strategies for $P_\forall$ explicitly,
  building up to a winning strategy.
- example

$$\exists x \forall u \exists y \forall v (x \vee u \vee y \vee \neg v)(x \vee u \vee \neg y \vee v)(\neg x)$$

$$\cfrac{\cfrac{\cfrac{(x \vee u \vee y \vee \neg v)}{(x \vee y), (u=0, v=1)} \qquad \cfrac{(x \vee u \vee \neg y \vee v)}{(x \vee \neg y), (u=0, v=0)}}{(x), (u=0, v=\text{if } y=0 \text{ then } 1 \text{ else } 0)} \qquad (\neg x), ()}{(\Box), (u=0, v=\text{if } y=0 \text{ then } 1 \text{ else } 0)}$$

A new QBF proof system: MRes (cont'd)

- Syntax of lines in proof:

$$\underbrace{C}_{\text{clause over } X_\exists} \quad , \quad \underbrace{h_{u_1}, h_{u_2}, \ldots h_{u_s}}_{\text{a function for each } \ u \in X_\forall}$$

- For $u \in X_\forall$, the function h_u depends only on $x \in X_\exists$, $x < u$.
- Desired Invariant (expressing partial winning strategy):
  For all assignments α to $X_\exists$, if α falsifies C,
  then $\alpha, \vec{h}_u(\alpha)$ falsifies some axiom clause.
- If $C = \Box$, this gives a $P_\forall$ winning strategy – soundness.
- Rule:
  - Resolution on clause part, provided
    for each $u \in X_\forall$, h_u^1 and h_u^2 "compatible".
  - Augmenting functions through if-then-else.

Proving completeness

- Fix a $P_\forall$ winning strategy $\vec{h}$.
- Start with trivial / constant strategies at initial clauses.
- Perform appropriate resolutions to build up $\vec{h}$.
- Show: all required resolutions satisfy compatibility.

How to represent partial strategies?

- Crucially affects refutation size.
- If-then-else augmentation naturally leads to decision trees.
  Too large for many strategies.
- Circuits, Branching Programs, Binary Decision Diagrams BDDs: more compact.
  But hard to check compatibility.

How to represent partial strategies?

- Crucially affects refutation size.
- If-then-else augmentation naturally leads to decision trees.
  Too large for many strategies.
- Circuits, Branching Programs, Binary Decision Diagrams BDDs: more compact.
  But hard to check compatibility.
- Our choice:

  Binary Decision Diagrams
  +
  a more stringent compatibility check.

- Even though functional equivalence sufficient for soundness, we require isomorphism.
  Easy to check for BDDs.
  Keeps strategy-storage overhead under control.

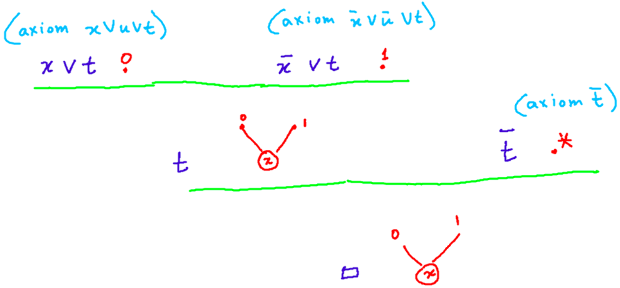
A refutation in MergeRes

$$\exists x\ \forall u\ \exists t\ \ (x \vee u \vee t)(\bar{x} \vee \bar{u} \vee t)(\bar{t})$$

A refutation in MergeRes

$$\exists x \; \forall u \; \exists t \quad (x \vee u \vee t)(\bar{x} \vee \bar{u} \vee t)(\bar{t})$$

Refutation:

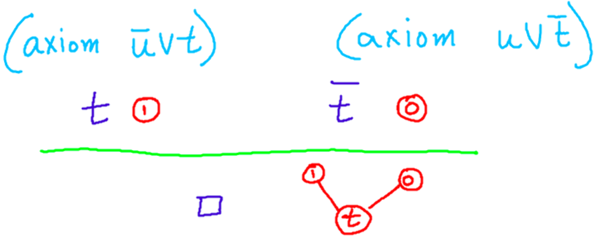


A non-refutation in MergeRes

A true QBF: $\forall u \; \exists t \quad (\bar{u} \vee t)(u \vee \bar{t})$.

A non-refutation in MergeRes

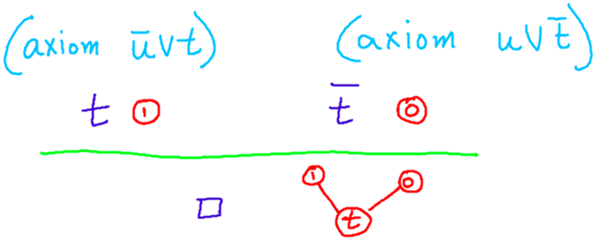
A true QBF: $\forall u\ \exists t\ \ (\bar{u} \vee t)(u \vee \bar{t})$.
An unsound refutation?



A non-refutation in MergeRes

A true QBF: $\forall u \; \exists t \;\; (\bar{u} \vee t)(u \vee \bar{t})$.

An unsound refutation?



Not a valid refutation.

u cannot depend on t because u is quantified before t.

Where MRes scores ... (1)

The Equality Formulas $EQ_n : \exists x_1, \ldots, x_n, \forall u_1, \ldots, u_n, \exists t_1, \ldots, t_n$

$$\begin{array}{rll} P_i : & (x_i \vee u_i \vee t_i) & i \in [n] \\ N_i : & (\overline{x}_i \vee \overline{u}_i \vee t_i) & i \in [n] \\ L : & (\overline{t}_1, \ldots, \overline{t}_n) & \end{array}$$

Where MRes scores ... (1)

The Equality Formulas $EQ_n : \exists x_1, \ldots, x_n, \forall u_1, \ldots, u_n, \exists t_1, \ldots, t_n$

$$\begin{array}{rll} P_i : & (x_i \vee u_i \vee t_i) & i \in [n] \\ N_i : & (\overline{x}_i \vee \overline{u}_i \vee t_i) & i \in [n] \\ L : & (\overline{t}_1, \ldots, \overline{t}_n) & \end{array}$$

- False QBF. $\forall$-player has unique winning strategy $u_i = x_i \forall i$.

Where MRes scores ... (1)

The Equality Formulas $EQ_n : \exists x_1, \ldots, x_n, \forall u_1, \ldots, u_n, \exists t_1, \ldots, t_n$

$$\begin{array}{rll} P_i : & (x_i \vee u_i \vee t_i) & i \in [n] \\ N_i : & (\overline{x}_i \vee \overline{u}_i \vee t_i) & i \in [n] \\ L : & (\overline{t}_1, \ldots, \overline{t}_n) & \end{array}$$

- False QBF. $\forall$-player has unique winning strategy $u_i = x_i \forall i$.
- Hard in expansion-based systems $\forall$Exp+Res and IR.
- Hard in reduction-based systems Q-Res and QU-Res.
- Easy in LDQRes (even reductionless LDQRes)

Where MRes scores ... (1)

The Equality Formulas $EQ_n : \exists x_1, \ldots, x_n, \forall u_1, \ldots, u_n, \exists t_1, \ldots, t_n$

$$\begin{array}{rll} P_i : & (x_i \vee u_i \vee t_i) & i \in [n] \\ N_i : & (\overline{x}_i \vee \overline{u}_i \vee t_i) & i \in [n] \\ L : & (\overline{t}_1, \ldots, \overline{t}_n) & \end{array}$$

- False QBF. $\forall$-player has unique winning strategy $u_i = x_i \forall i$.
- Hard in expansion-based systems $\forall$Exp+Res and IR.
- Hard in reduction-based systems Q-Res and QU-Res.
- Easy in LDQRes (even reductionless LDQRes)
- Easy in MergeRes ... even regular and treelike

Where MRes scores ... (2)

The SquaredEquality Formulas

$SqEQ_n : \exists x_1, \ldots, x_n, \exists y_1, \ldots, y_n, \forall u_1, \ldots, u_n, \forall v_1, \ldots, v_n, \exists \{t_{i,j} \mid i, j \in [n]\}$

$$
\begin{array}{ll}
(x_i \vee u_i \vee y_j \vee v_j \vee t_{i,j}) & i, j \in [n] \\
(x_i \vee u_i \vee \bar{y}_j \vee \bar{v}_j \vee t_{i,j}) & i, j \in [n] \\
(\bar{x}_i \vee \bar{u}_i \vee y_j \vee v_j \vee t_{i,j}) & i, j \in [n] \\
(\bar{x}_i \vee \bar{u}_i \vee \bar{y}_j \vee \bar{v}_j \vee t_{i,j}) & i, j \in [n] \\
\bigvee_{i,j} \bar{t}_{i,j} &
\end{array}
$$

- False QBF. $\forall$-player has unique winning strategy $u_i = x_i \forall i$, $v_j = y_j \forall j$.

Where MRes scores ... (2)

The SquaredEquality Formulas

$SqEQ_n : \exists x_1, \ldots, x_n, \exists y_1, \ldots, y_n, \forall u_1, \ldots, u_n, \forall v_1, \ldots, v_n, \exists \{t_{i,j} \mid i,j \in [n]\}$

$$\begin{array}{ll} (x_i \vee u_i \vee y_j \vee v_j \vee t_{i,j}) & i,j \in [n] \\ (x_i \vee u_i \vee \bar{y}_j \vee \bar{v}_j \vee t_{i,j}) & i,j \in [n] \\ (\bar{x}_i \vee \bar{u}_i \vee y_j \vee v_j \vee t_{i,j}) & i,j \in [n] \\ (\bar{x}_i \vee \bar{u}_i \vee \bar{y}_j \vee \bar{v}_j \vee t_{i,j}) & i,j \in [n] \\ \bigvee_{i,j} \bar{t}_{i,j} & \end{array}$$

- False QBF. $\forall$-player has unique winning strategy $u_i = x_i \forall i$, $v_j = y_j \forall j$.
- Hard in reductionless LDQRes
- Easy in MergeRes ... even regular and treelike.

Where MRes fails ... (1)

- MRes stores $P_\forall$ winning strategies explictly. Hence

$$\text{No small representation in underlying model} \\ \Downarrow \\ \text{no short refutation}$$

- If function f is
  - hard in underlying model, but
  - has small circuit C.

  then we can craft a small false QBF

$$Q_{f,C} : \exists\vec{x}\forall u\exists\vec{t} \quad (u \neq t_m)(\vec{t} \text{ encodes gate values of } C(\vec{x}))$$

  Unique winning strategy for $P_\forall$ is $u = f(\vec{x})$.

  Hence $Q_{f,C}$ has no short refutations.

Where MRes fails ... (2)

- Tree-like MRes: strategy representions are decision trees.

  Large decision tree size for every $P_\forall$ winning strategy
  $$\Downarrow$$
  No short tree-like MRes refutations.

  eg QParity.
- Regular MRes: strategy representions are read-once BDDs.

  Large read-once BDD size for every $P_\forall$ winning strategy
  $$\Downarrow$$
  No short regular MRes refutations.
- General MRes? No unconditional lower bounds known for BDD size.

Where MRes fails ... (3)

- Lower bounds for general MRes: find another weakness.

Where MRes fails ... (3)

- Lower bounds for general MRes: find another weakness.
- To make verification easy, we impose isomorphim requirement – more stringent than needed for soundness.
- Building isomorphic partial strategies not always easy.

Where MRes fails ... (3)

- Lower bounds for general MRes: find another weakness.
- To make verification easy, we impose isomorphim requirement – more stringent than needed for soundness.
- Building isomorphic partial strategies not always easy.
- We show: the KBKF-lq formulas, easy in QURes but hard for LDQRes, are also hard for MRes.

Some new strengths of MRes ... (1)

Formula	tweak	hardness
QParity		QURes
LQParity	duplicate clauses $C \to C \vee z, C \vee \neg z$	LDQRes
QUParity	duplicate z $z \to z_1 \vee z_2;\ \neg z \to \neg z_1 \vee \neg z_2$	$\mathrm{LQU}^+\mathrm{Res}$
MParity	weaken some clauses add some new clauses	$\mathrm{LQU}^+\mathrm{Res}$ easy for MRes

Some new strengths of MRes ... (2)

Formula	hardness
KBKF	QRes
KBKF-lq	QRes, LDQRes, IRM, MRes
KBKF-lq-weak	easy in MRes
KBKF-lq-split	hard for IRM easy in MRes

A new weakness of MRes

KBKF-lq	hard for MRes
KBKF-lq-split	easy in MRes

- But KBKF-lq is a restriction of KBKF-lq-split.
- So MRes is not "closed under restrictions".

  Shortest refutation size of $\Phi|_{x=b}$ $>$ Shortest refutation size of Φ.

  MRes is an unnatural proof system.

  Perhaps not suited for implementing as solver.

Overcoming the weakness with weakening?

KBKF-lq	hard for MRes
KBKF-lq-weak	easy in MRes

- But KBKF-lq-weak is just a weakening of KBKF-lq.
- Why not add a weakening rule to the proof system?
- Weakening itself needs to be defined carefully!

Types of weakening

	Clause	line
	D	$(C, h_{u_1}, h_{u_2}, \ldots, h_{u_s})$.
For $x \in X_\exists$	Weaken to $D \vee x$	$(C \vee x, h_{u_1}, h_{u_2}, \ldots, h_{u_s})$.
For $u \in X_\forall$	Weaken to $D \vee u$	$(C, h'_{u_1}, h'_{u_2}, \ldots, h'_{u_s})$. For $u_i \neq u$, $h'_{u_i} = h_{u_i}$. h_u should be $*$; h'_u can be 0 or 1.

Types of weakening

	Clause	line
	D	$(C, h_{u_1}, h_{u_2}, \ldots, h_{u_s})$.
For $x \in X_\exists$	Weaken to $D \vee x$	$(C \vee x, h_{u_1}, h_{u_2}, \ldots, h_{u_s})$.
For $u \in X_\forall$	Weaken to $D \vee u$	$(C, h'_{u_1}, h'_{u_2}, \ldots, h'_{u_s})$. For $u_i \neq u$, $h'_{u_i} = h_{u_i}$. h_u should be $*$; h'_u can be 0 or 1.

- Invariant maintained.
- Note: Changing $h_u = *$ to any h'_u would be sound.
  But hard to analyse/control size.

Types of systems

- MRes: only merge resolution, no weakening.
- $\text{MResW}_\exists$: Merge resolution, only existential weakening.
- $\text{MResW}_\forall$: Merge resolution, only universal (strategy) weakening.
- MResW: Merge resolution, any weakening.

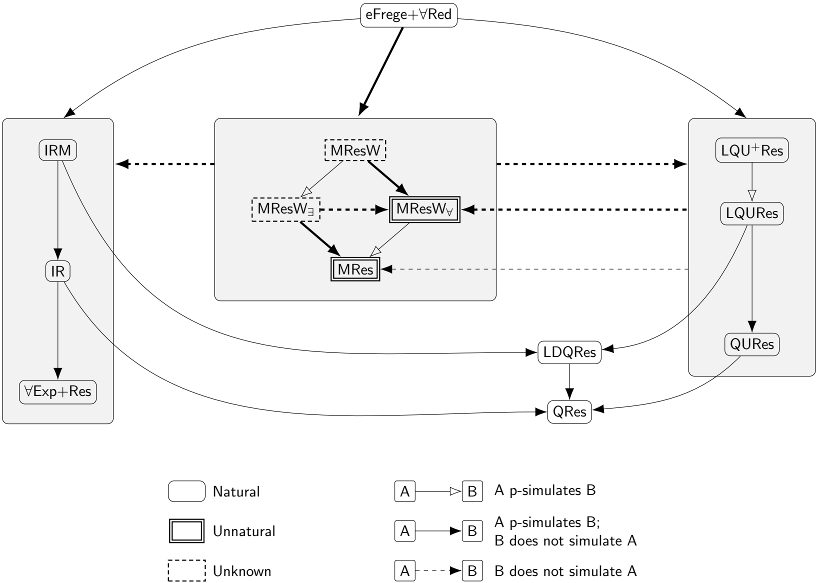
Types of systems

- MRes: only merge resolution, no weakening.
- $\text{MResW}_\exists$: Merge resolution, only existential weakening.
- $\text{MResW}_\forall$: Merge resolution, only universal (strategy) weakening.
- MResW: Merge resolution, any weakening.

We show:

- $\text{MRes}_\forall$ does not simulate $\text{MRes}_\exists$.
- Regular MRes does not simulate Regular $\text{MRes}_\forall$.
- eFrege+$\forall$Red simulates MResW.

The overall landscape



How else weakening helps

- MResW is sound and complete for Dependency QBF (DQBF), a more succinctly expressive formalism that is NEXPTIME-complete.
- MRes is provably not complete for DQBF.

  So weakening really helps.

Summary

- $\forall$-Expansion, $\forall$-Reduction, existing paradigms for resolution-based QBF proof systems.

  Merge-Resolution: a new approach.
- Builds strategies into proofs with compact representations.
- Lines in the proof have a clear semantic meaning.
- Enables some sound inference steps blocked in existing systems.
- Exponentially more powerful than LQU$^+$Res, IRM on some formulas.
- Exponentially weaker than LQU$^+$Res on other formulas.
- Unnatural: restrictions may need exponentially larger proofs.
- Weakening adds power for QBFs, also makes the system complete for DQBFs.

Questions

- Can other representations of partial strategies be used more advantageously?
  Two conflicting requirements: succinct representations, and ease of checking equivalence.
- Can the search for a $P_\forall$ winning strategy,
  and the goal of preserving a $P_\exists$ winning strategy,
  somehow be interleaved to any advantage?

Questions

- Can other representations of partial strategies be used more advantageously?
  Two conflicting requirements: succinct representations, and ease of checking equivalence.
- Can the search for a $P_\forall$ winning strategy,
  and the goal of preserving a $P_\exists$ winning strategy,
  somehow be interleaved to any advantage?

Thank you