Dependency Quantified Boolean Formulas

Uwe Bubeck

Universität Paderborn

17.01.2013

Outline

- Introduction
- Models
- Dependency Quantification
- DQBF Subclasses
- Conclusion

Introduction

Quantified Boolean Formulas 1/2

QBF extends propositional logic by allowing universal and existential quantifiers over propositional variables.

Inductive definition:

1. Every propositional formula is a QBF.
2. If Φ is a QBF then $\forall x \Phi$ and $\exists y \Phi$ are also QBFs.
3. If Φ_1 and Φ_2 are QBFs then $\neg\Phi_1$, $\Phi_1 \wedge \Phi_2$ and $\Phi_1 \vee \Phi_2$ are also QBFs.

Quantified Boolean Formulas 2/2

In a closed QBF, every variable is quantified.

Semantics definition for closed QBF:

$\exists y\ \Phi(y)$ is true if and only if

$\Phi[y/0]$ is true or $\Phi[y/1]$ is true.

$\forall x\ \Phi(x)$ is true if and only if

$\Phi[x/0]$ is true and $\Phi[x/1]$ is true.

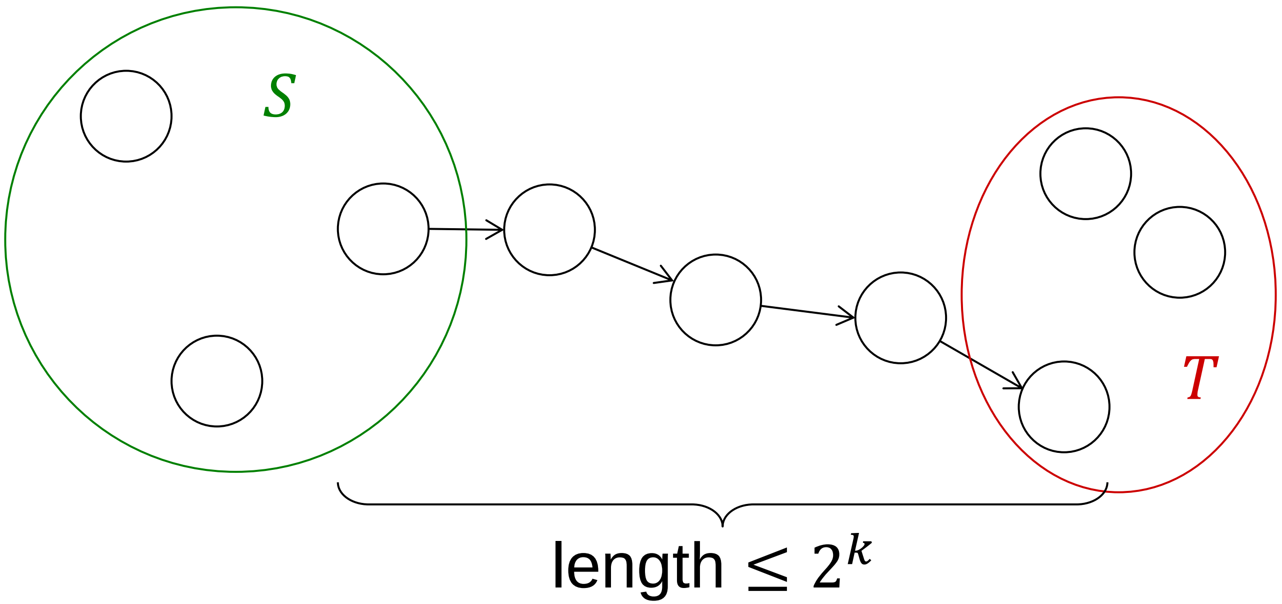
$\Rightarrow$ A closed QBF is

either true or false.

Bounded Reachability 1/4

Application: Bounded Reachability / S-T-Connectivity

Given a directed graph $G = (V, E)$, start nodes $S \subseteq V$, terminal nodes $T \subseteq V$ and bound $k \geq 0$, is there a path of length at most 2^k from some $s \in S$ to some $t \in T$?



Bounded Reachability 2/4

In Bounded Model Checking, vertices are typically binary vectors ($V = \{0,1\}^n$), and the edges are given by a transition relation δ:

$\delta(\boldsymbol{u}, \boldsymbol{v}) = 1$ iff there is an edge from $\boldsymbol{u} = (u_1, \dots, u_n)$ to $\boldsymbol{v} = (v_1, \dots, v_n)$.

If δ is encoded as a propositional formula, the whole reachability test can be formulated in propositional logic:

$$S(\boldsymbol{v}_0) \wedge T\left(\boldsymbol{v}_{2^k}\right) \bigwedge_{i=0}^{2^k-1} \delta(\boldsymbol{v}_i, \boldsymbol{v}_{i+1})$$

Bounded Reachability 3/4

$$S(\boldsymbol{v}_0) \wedge T(\boldsymbol{v}_{2^k}) \bigwedge_{i=0}^{2^k-1} \delta(\boldsymbol{v}_i, \boldsymbol{v}_{i+1})$$

Problem: many copies of δ

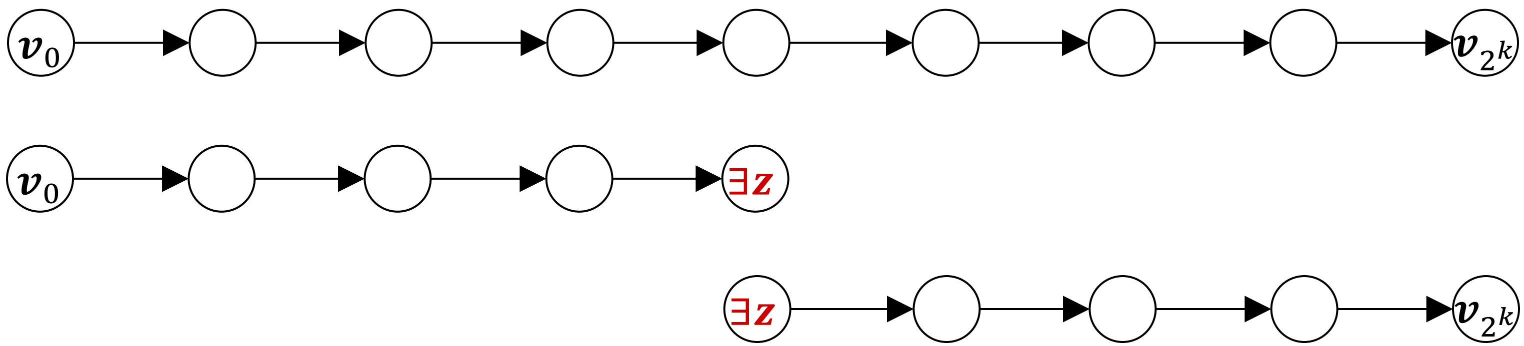
Compress conjunctions of renamings / instantiations by universal variables:

$$S(\boldsymbol{v}_0) \wedge T(\boldsymbol{v}_{2^k}) \wedge \forall \boldsymbol{u} \forall \boldsymbol{w} \left(\left(\bigvee_{i=0}^{2^k-1} \left((\boldsymbol{u} = \boldsymbol{v}_i) \wedge (\boldsymbol{w} = \boldsymbol{v}_{i+1}) \right) \right) \rightarrow \delta(\boldsymbol{u}, \boldsymbol{w}) \right)$$

[Dershowitz et al., 2005], [Meyer/Stockmeyer, 1973]

Bounded Reachability 4/4

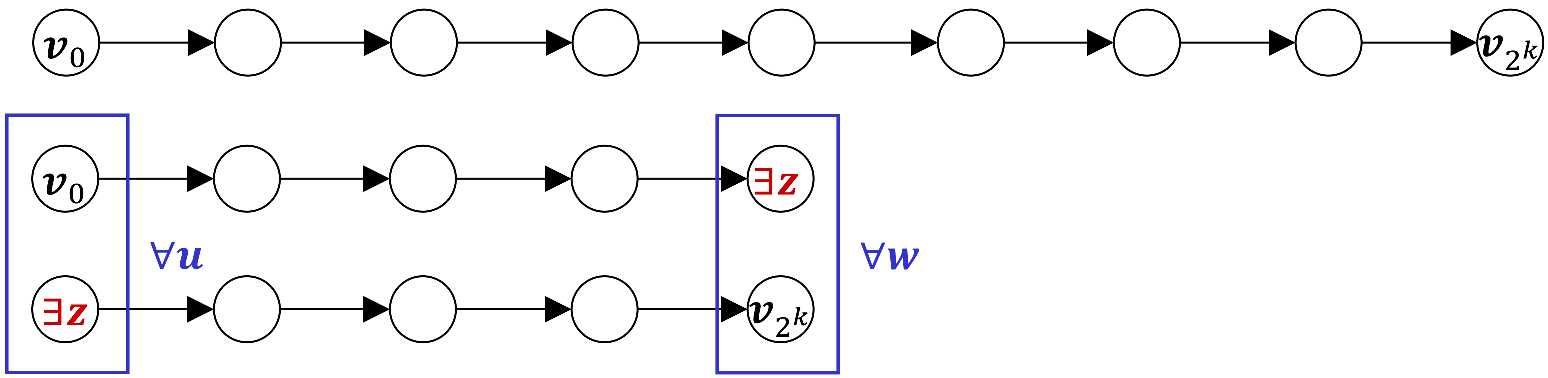
Even more compact: iterative squaring



$$
\begin{aligned}
\delta_{2^k}(\boldsymbol{a},\boldsymbol{b}) &:= \exists \boldsymbol{z}\, \delta_{2^{k-1}}(\boldsymbol{a},\boldsymbol{z}) \wedge \delta_{2^{k-1}}(\boldsymbol{z},\boldsymbol{b}) \\
&\vdots \\
\delta_1(\boldsymbol{a},\boldsymbol{b}) &:= \delta(\boldsymbol{a},\boldsymbol{b})
\end{aligned}
$$

Bounded Reachability 4/4

Even more compact: iterative squaring



$$\delta_{2^k}(\boldsymbol{a},\boldsymbol{b}) \coloneqq \exists \boldsymbol{z} \forall \boldsymbol{u} \forall \boldsymbol{w} \left(\left((\boldsymbol{u} = \boldsymbol{a}) \wedge (\boldsymbol{w} = \boldsymbol{z}) \right) \vee \left((\boldsymbol{u} = \boldsymbol{z}) \wedge (\boldsymbol{w} = \boldsymbol{b}) \right) \right) \rightarrow \delta_{2^{k-1}}(\boldsymbol{u},\boldsymbol{w})$$

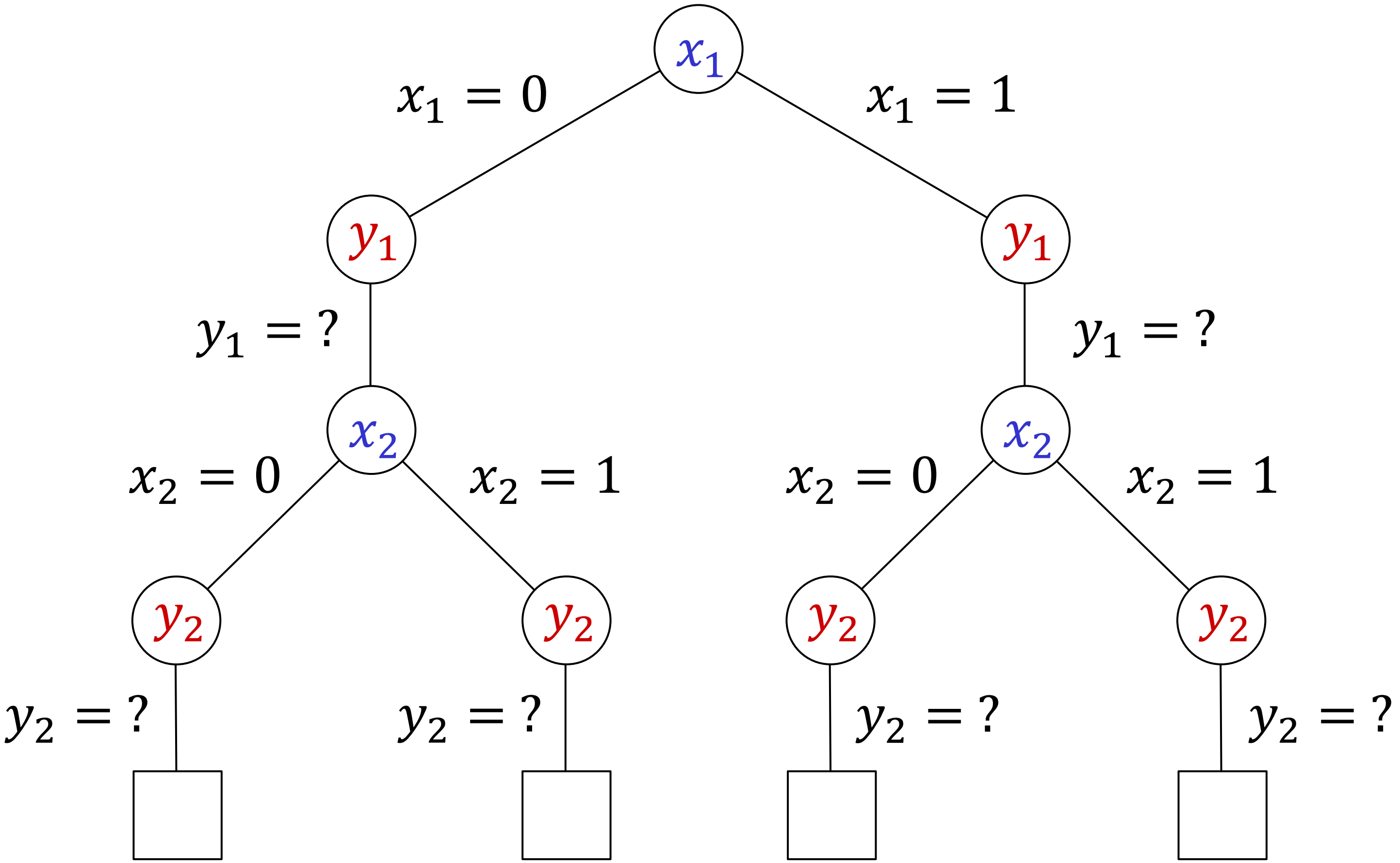
By the existential quantifier, the choice of the middle point becomes local to each piece.

[Meyer/Stockmeyer, 1973]

Models

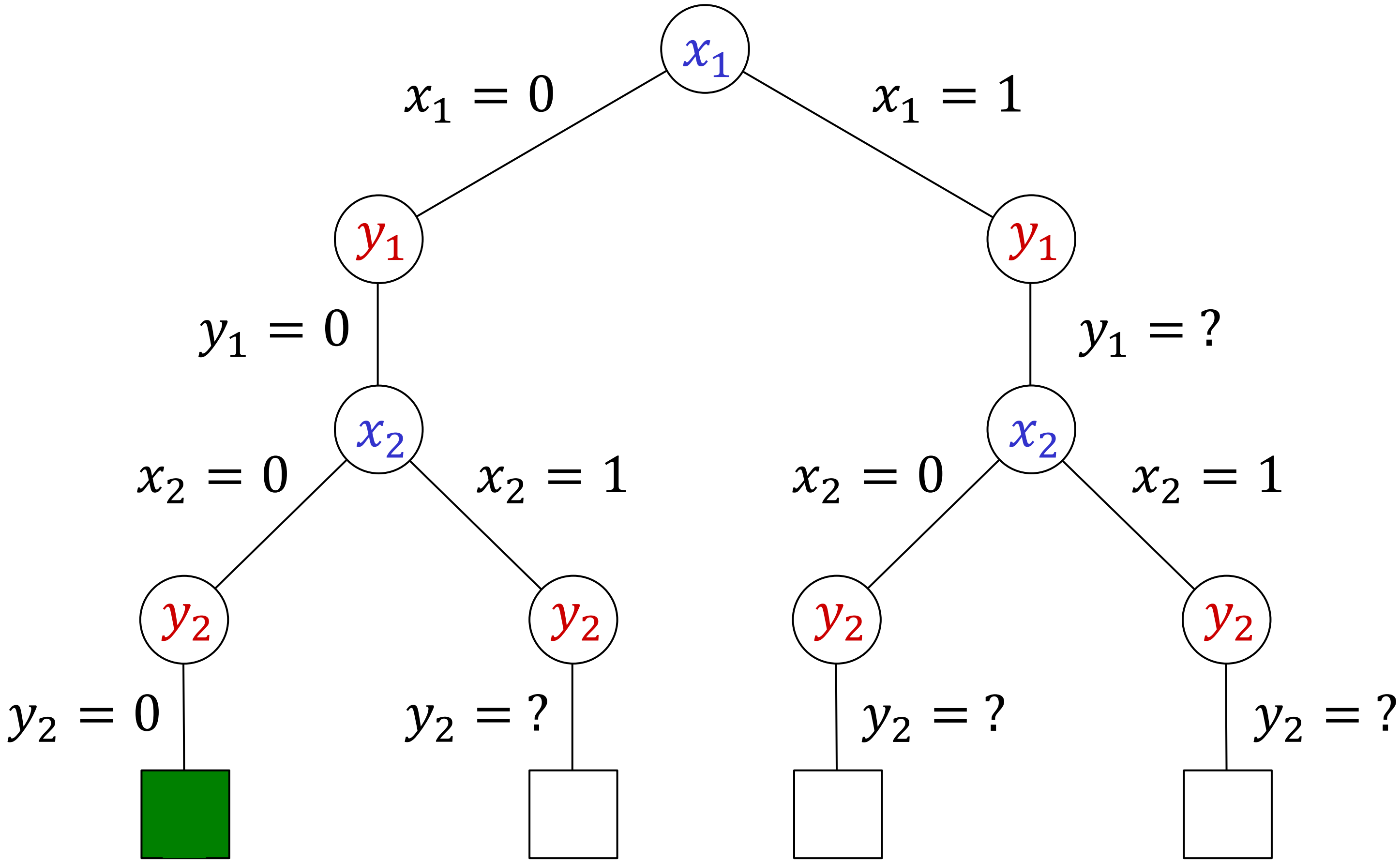
Tree Models

$\forall x_1 \exists y_1 \forall x_2 \exists y_2 \ (x_1 \vee \neg y_1) \wedge (\neg x_1 \vee y_2) \wedge (y_1 \vee x_2 \vee \neg y_2) \wedge (\neg x_2 \vee y_2)$



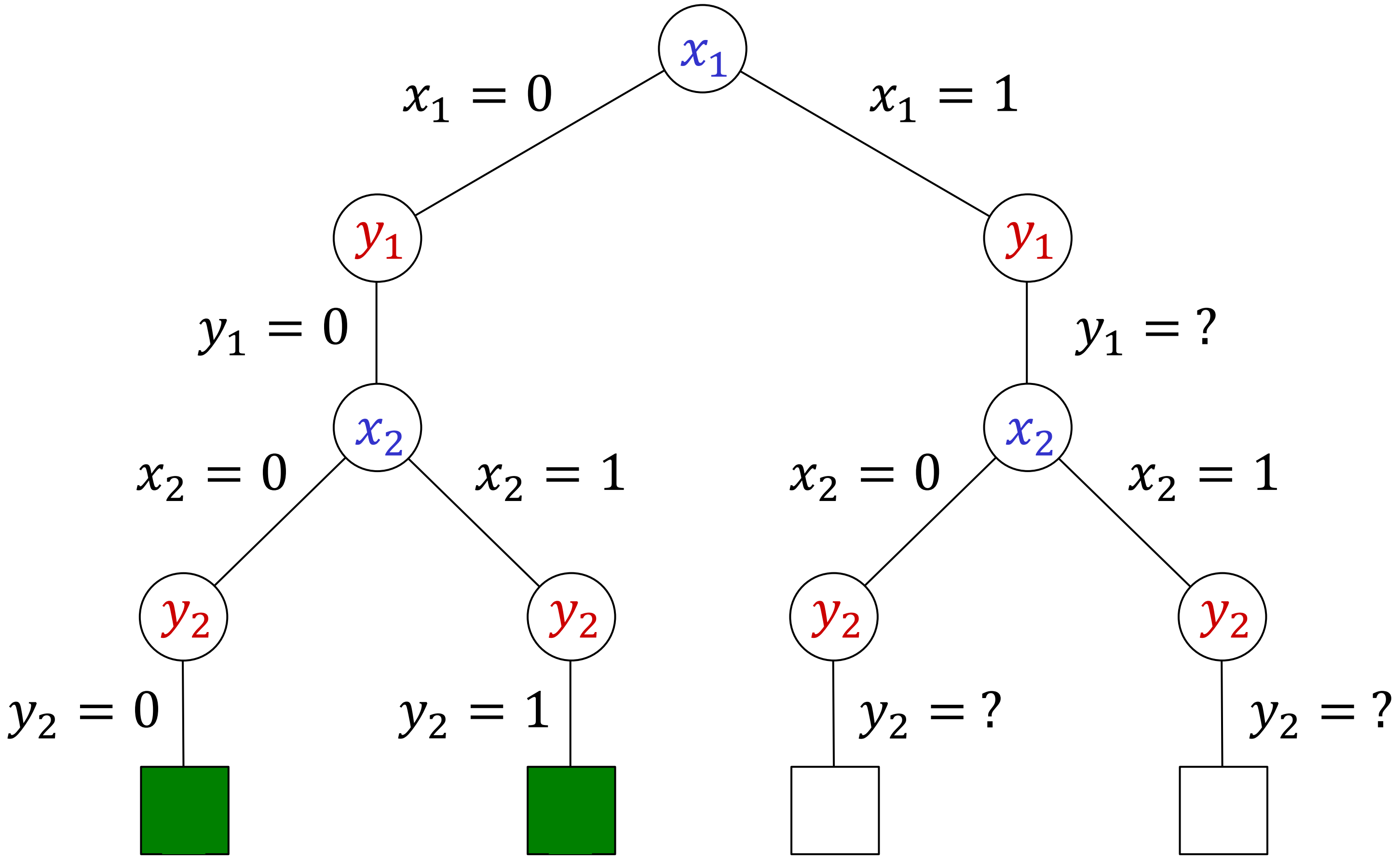
Tree Models

$\forall x_1 \exists y_1 \forall x_2 \exists y_2 \ (x_1 \lor \neg y_1) \land (\neg x_1 \lor y_2) \land (y_1 \lor x_2 \lor \neg y_2) \land (\neg x_2 \lor y_2)$



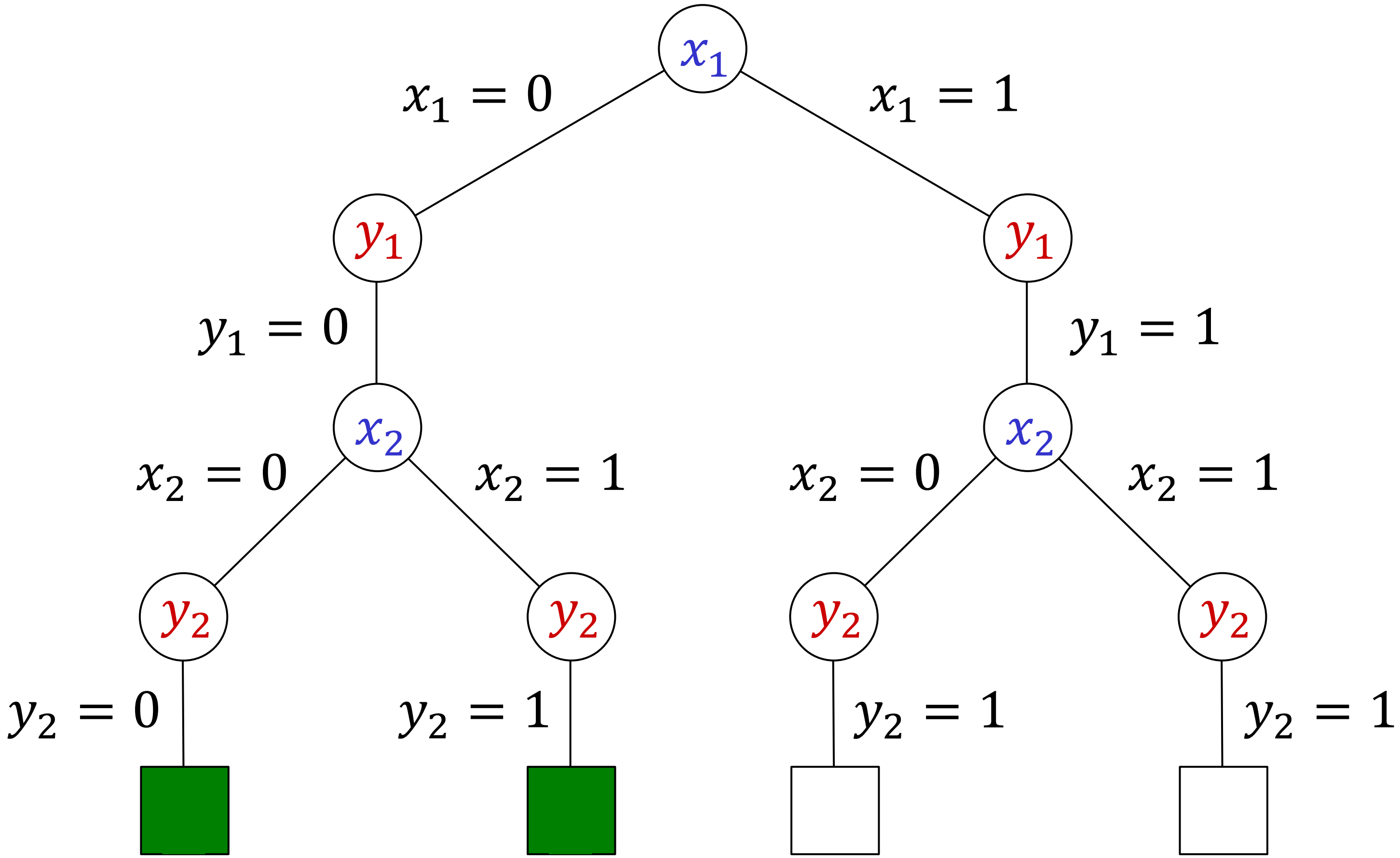
Tree Models

$$\forall x_1 \exists y_1 \forall x_2 \exists y_2 \; (x_1 \vee \neg y_1) \wedge (\neg x_1 \vee y_2) \wedge (y_1 \vee x_2 \vee \neg y_2) \wedge (\neg x_2 \vee y_2)$$



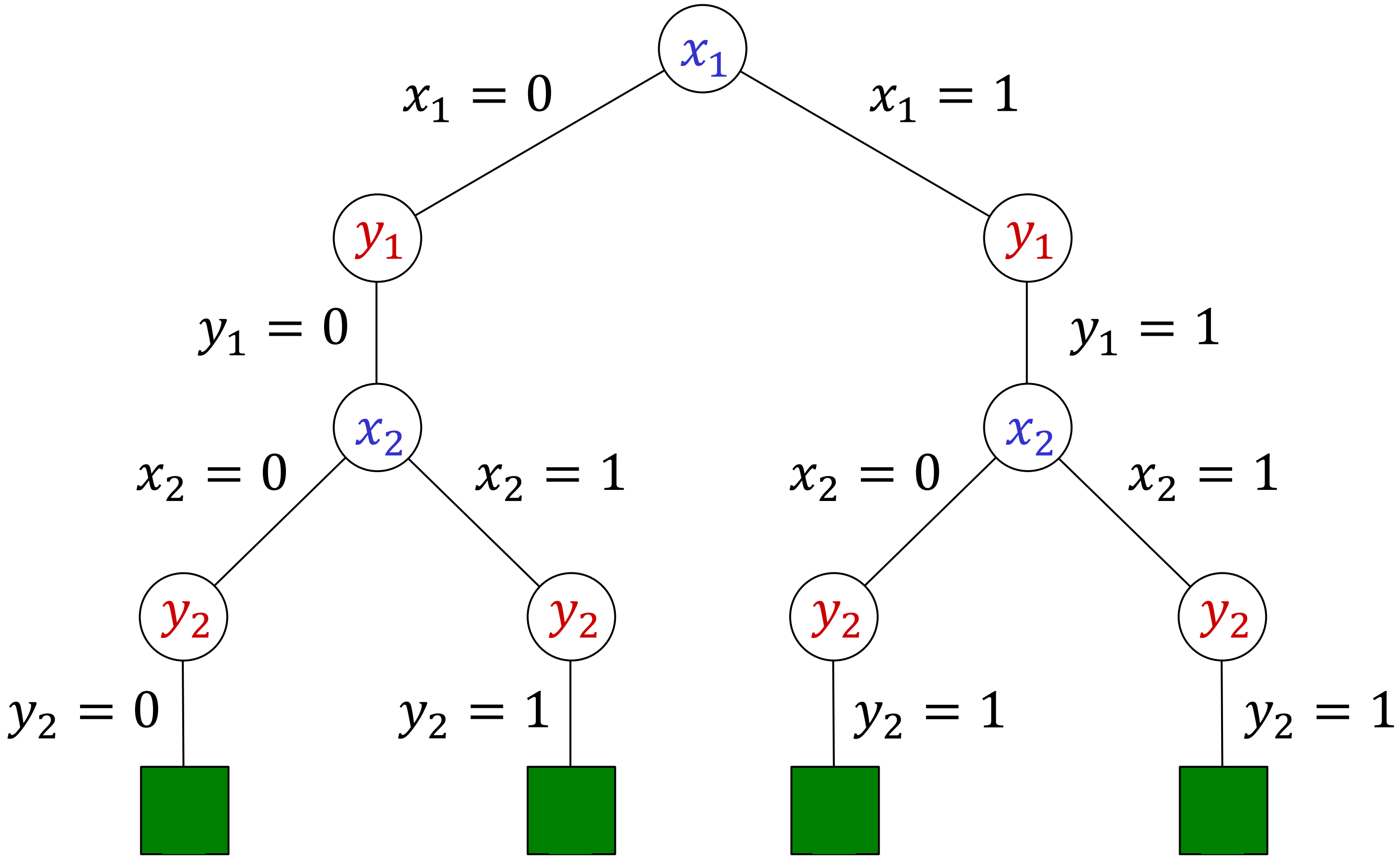
Tree Models

$\forall x_1 \exists y_1 \forall x_2 \exists y_2\ (x_1 \vee \neg y_1) \wedge (\neg x_1 \vee y_2) \wedge (y_1 \vee x_2 \vee \neg y_2) \wedge (\neg x_2 \vee y_2)$

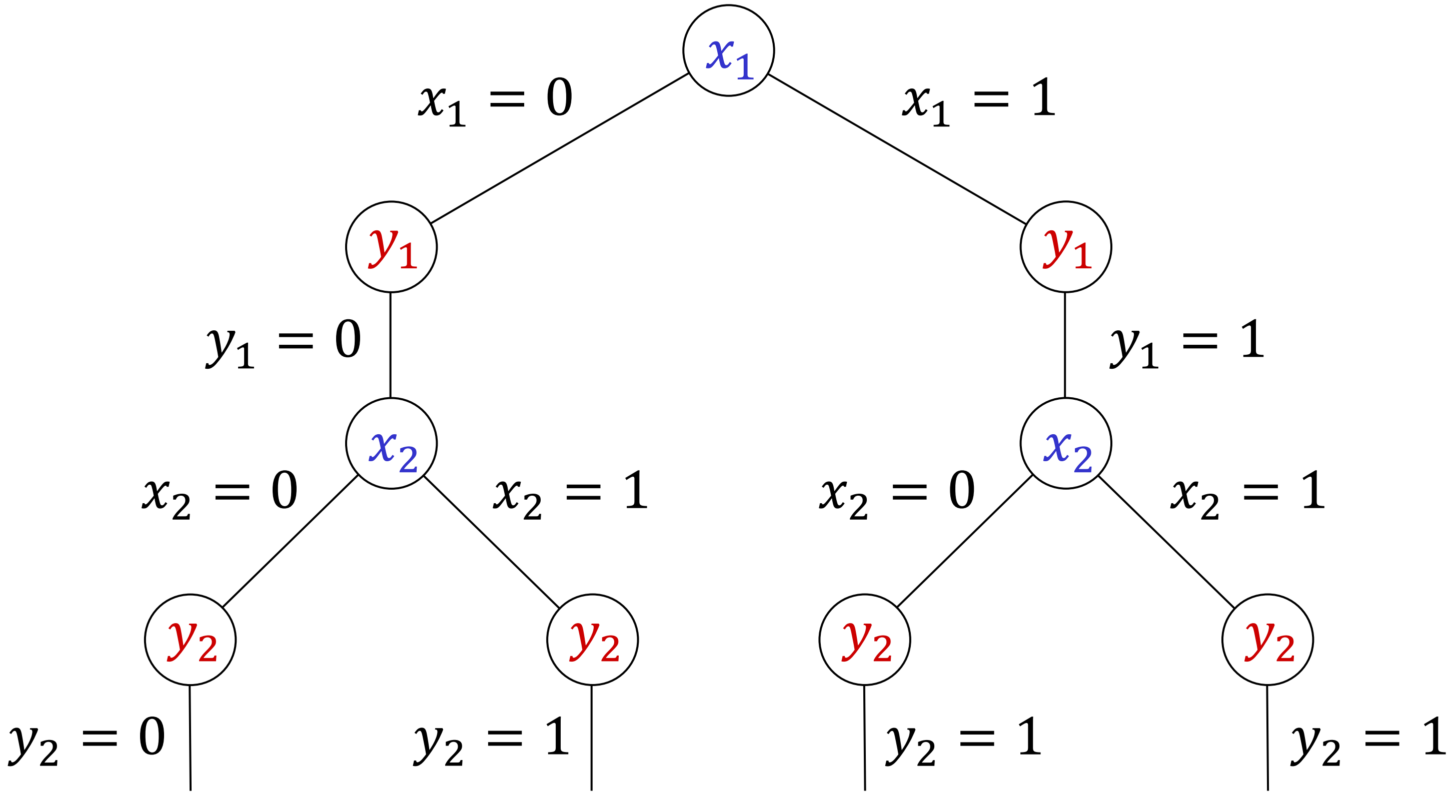


Tree Models

$\forall x_1 \exists y_1 \forall x_2 \exists y_2\ (x_1 \vee \neg y_1) \wedge (\neg x_1 \vee y_2) \wedge (y_1 \vee x_2 \vee \neg y_2) \wedge (\neg x_2 \vee y_2)$



Function Models 1/2



We can describe the choices for y_1 and y_2 by Skolem or model functions $f_{y_1}(x_1) = x_1$ and $f_{y_2}(x_1, x_2) = x_1 \vee x_2$.

Function Models 2/2

Theorem

A closed prenex QBF Φ with existential variables $y_1, \dots, y_m$ is true iff there exist $f_{y_1}, \dots, f_{y_m}$ such that:

1. Each f_{y_i} is a propositional formula over universal variables which are quantified further outside than y_i.

2. Simultaneous replacement $\Phi\left[y_1/f_{y_1}, \dots, y_m/f_{y_m}\right]$ of all variable occurrences with corresponding functions produces a true formula.

Dependency Quantification

Dependency Quantification 1/3

Motivation: overcome the tight correspondence between prefix order and arguments of the model functions.

Prenex QBF: $\forall x_1 \exists y_1 \forall x_2 \exists y_2 \forall x_3 \exists y_3\ \phi$

with model functions $f_{y_1}(x_1), f_{y_2}(x_1, x_2), f_{y_3}(x_1, x_2, x_3)$

and $\{x_1\} \subseteq \{x_1, x_2\} \subseteq \{x_1, x_2, x_3\}$.

Now DQBF: $\forall x_1 \forall x_2 \exists y_1(x_1) \exists y_2(x_2) \exists y_3(x_1, x_2)\ \phi$

with model functions $f_{y_1}(x_1), f_{y_2}(x_2), f_{y_3}(x_1, x_2)$

and $\{x_1\} \nsubseteq \{x_2\}$.

Dependency Quantification 2/3

A (closed) DQBF is a formula of the form

$\Phi = \forall x_1 \ldots \forall x_n \exists y_1(x_{d_{1,1}}, \ldots, x_{d_{1,n_1}}) \ldots \exists y_m(x_{d_{m,1}}, \ldots, x_{d_{m,n_m}})\, \phi$

where $\{d_{i,1}, \ldots, d_{i,n_i}\} \subseteq \{1, \ldots, n\}$ are the dependencies of y_i,

and ϕ is a propositional matrix over $x_1, \ldots, x_n, y_1, \ldots, y_m$.

Semantics Definition

Φ is true if and only if there exist $f_{y_1}, \ldots, f_{y_m}$ such that:

1. Each f_{y_i} is a propositional formula over $x_{d_{i,1}}, \ldots, x_{d_{i,n_i}}$.
2. $\Phi[y_1/f_{y_1}, \ldots, y_m/f_{y_m}]$ is true.

Dependency Quantification 3/3

Generalization to DQBF with free variables [Bubeck, 2010]

A DQBF with free variables $z_1, \dots, z_r$ is a formula

$\Phi = \forall x_1 \dots \forall x_n \exists y_1(x_{d_{1,1}}, \dots, x_{d_{1,n_1}}) \dots \exists y_m(x_{d_{m,1}}, \dots, x_{d_{m,n_m}})\ \phi$

where $\{d_{i,1}, \dots, d_{i,n_i}\} \subseteq \{1, \dots, n\}$, and ϕ is a propositional matrix over $x_1, \dots, x_n, y_1, \dots, y_m$ and $z_1, \dots, z_r$.

Semantics Definition

$\Phi \in$ DQBF with free variables $z_1, \dots, z_r$ is satisfiable iff there exists a truth assignment $(\tau(z_1), \dots, \tau(z_r)) \in \{0,1\}^r$ such that $\Phi[z_1/\tau(z_1), \dots, z_r/\tau(z_r)]$ is true.

DQBF Satisfiability 1/2

The semantics of QBF is defined inductively as in the tree models. For DQBF, direct recursive evaluation without storing (parts of) model functions seems not possible.

Workaround [Fröhlich et al., 2012]

Whenever choosing $\exists y_i(x_{d_{i,1}}, \dots, x_{d_{i,n_i}})$ in DPLL style, add a Skolem clause $(l(x_{d_{i,1}}) \wedge \dots \wedge l(x_{d_{i,n_i}})) \rightarrow l(y_i)$ where $l(v) = v$ or $l(v) = \neg v$ according to the current assignment to v.

DQBF Satisfiability 2/2

Theorem

The DQBF satisfiability problem is NEXPTIME-complete.

[Peterson / Reif, 1979]

This even holds for relatively simple prefixes of the form

$$\forall \boldsymbol{u} \forall \boldsymbol{v} \exists \boldsymbol{y}(\boldsymbol{u}) \exists \boldsymbol{z}(\boldsymbol{v})$$

where $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{y}$ and $\boldsymbol{z}$ are (disjoint) tuples of variables.

Surprising at first, since we can have non-prenex QBF

$$\big(\forall \boldsymbol{u} \exists \boldsymbol{y}\ \phi(\boldsymbol{u}, \boldsymbol{y})\big) \land \big(\forall \boldsymbol{v} \exists \boldsymbol{z}\ \psi(\boldsymbol{v}, \boldsymbol{z})\big)$$

$$\approx \forall \boldsymbol{u} \forall \boldsymbol{v} \exists \boldsymbol{y} \exists \boldsymbol{z}\ \big(\phi(\boldsymbol{u}, \boldsymbol{y}) \land \psi(\boldsymbol{v}, \boldsymbol{z})\big)$$

DQBF Encodings 1/6

Additional restriction of non-prenex QBF:

variables from disjoint quantifier scopes cannot occur in common subformulas:

$$\big(\forall \boldsymbol{u} \exists \boldsymbol{y}\ \phi(\boldsymbol{u}, \boldsymbol{y})\big) \land (\forall \boldsymbol{v} \exists \boldsymbol{z}\ \psi(\boldsymbol{v}, \boldsymbol{z}) \land \tau(\boldsymbol{y}, \boldsymbol{z}))$$

not possible

Why combine „unrelated“ variables in one subformula?

DQBF Encodings 2/6

Alternative modeling approach for bounded reachability:

Two-player game where

- universal player presents a step counter $\boldsymbol{c} = (c_1, \dots, c_k)$,
- existential player must find corresponding $\boldsymbol{u}$ and $\boldsymbol{v}$ so that $(\boldsymbol{c} = 0) \rightarrow S(\boldsymbol{u})$, $(\boldsymbol{c} = 2^k - 1) \rightarrow T(\boldsymbol{v})$ and $\delta(\boldsymbol{u}, \boldsymbol{v})$.

QBF formulation:

$$\forall \boldsymbol{c} \exists \boldsymbol{u} \exists \boldsymbol{v} \left((\boldsymbol{c} = 0) \rightarrow S(\boldsymbol{u}) \right) \wedge \left(\left(\boldsymbol{c} = 2^k - 1 \right) \rightarrow T(\boldsymbol{v}) \right) \wedge \delta(\boldsymbol{u}, \boldsymbol{v})$$

$\longrightarrow$ Clearly flawed: does not enforce a continuous path.

DQBF Encodings 3/6

Use two existential players and two counters:

- If $\boldsymbol{c}^{(2)} = \boldsymbol{c}^{(1)}$, both existential players must behave identically.
- If $\boldsymbol{c}^{(2)} = \boldsymbol{c}^{(1)} + 1$, second player continues where first player stopped.

$$\forall \boldsymbol{c}^{(1)} \exists \boldsymbol{u}^{(1)} \exists \boldsymbol{v}^{(1)} \forall \boldsymbol{c}^{(2)} \exists \boldsymbol{u}^{(2)} \exists \boldsymbol{v}^{(2)}$$

$$\big((\boldsymbol{c}^{(2)} = \boldsymbol{c}^{(1)}) \rightarrow (\boldsymbol{u}^{(1)} = \boldsymbol{u}^{(2)}) \land (\boldsymbol{v}^{(1)} = \boldsymbol{v}^{(2)}) \big) \land$$

$$\big((\boldsymbol{c}^{(2)} = \boldsymbol{c}^{(1)} + 1) \rightarrow (\boldsymbol{v}^{(1)} = \boldsymbol{u}^{(2)}) \big) \land$$

$$\big((\boldsymbol{c}^{(1)} = 0) \rightarrow S(\boldsymbol{u}^{(1)}) \big) \land \big((\boldsymbol{c}^{(1)} = 2^k - 1) \rightarrow T(\boldsymbol{v}^{(1)}) \big) \land \delta(\boldsymbol{u}^{(1)}, \boldsymbol{v}^{(1)})$$

DQBF Encodings 4/6

$$\forall \boldsymbol{c}^{(1)} \exists \boldsymbol{u}^{(1)} \exists \boldsymbol{v}^{(1)} \forall \boldsymbol{c}^{(2)} \exists \boldsymbol{u}^{(2)} \exists \boldsymbol{v}^{(2)}$$

$$\left((\boldsymbol{c}^{(2)} = \boldsymbol{c}^{(1)}) \rightarrow (\boldsymbol{u}^{(1)} = \boldsymbol{u}^{(2)}) \wedge (\boldsymbol{v}^{(1)} = \boldsymbol{v}^{(2)})\right) \wedge$$

$$\left((\boldsymbol{c}^{(2)} = \boldsymbol{c}^{(1)} + 1) \rightarrow (\boldsymbol{v}^{(1)} = \boldsymbol{u}^{(2)})\right) \wedge$$

$$\left((\boldsymbol{c}^{(1)} = 0) \rightarrow S(\boldsymbol{u}^{(1)})\right) \wedge \left((\boldsymbol{c}^{(1)} = 2^k - 1) \rightarrow T(\boldsymbol{v}^{(1)})\right) \wedge \delta\left(\boldsymbol{u}^{(1)}, \boldsymbol{v}^{(1)}\right)$$

Since $\boldsymbol{u}^{(2)}$ and $\boldsymbol{v}^{(2)}$ also depend on $\boldsymbol{c}^{(1)}$, second player can cheat by behaving differently:

$\boldsymbol{c}^{(1)} = \tau,\ \boldsymbol{c}^{(2)} = \tau + 1$:	$\boldsymbol{c}^{(1)} = \tau + 1,\ \boldsymbol{c}^{(2)} = \tau + 1$:
Player 1: $a \rightarrow b$	Player 1: $d \rightarrow e$
Player 2: $b \rightarrow c$	Player 2: $\cancel{b \rightarrow c}$ $d \rightarrow e$

DQBF Encodings 5/6

Choice of $\boldsymbol{u}^{(2)}$ and $\boldsymbol{v}^{(2)}$ should only depend on $\boldsymbol{c}^{(2)}$.

Solution: explicitly indicate dependencies in DQBF

$$\forall \boldsymbol{c}^{(1)} \forall \boldsymbol{c}^{(2)} \exists \boldsymbol{u}^{(1)}(\boldsymbol{c}^{(1)}) \exists \boldsymbol{v}^{(1)}(\boldsymbol{c}^{(1)})\ \exists \boldsymbol{u}^{(2)}(\boldsymbol{c}^{(2)}) \exists \boldsymbol{v}^{(2)}(\boldsymbol{c}^{(2)})$$
$$\left((\boldsymbol{c}^{(2)} = \boldsymbol{c}^{(1)}) \to (\boldsymbol{u}^{(1)} = \boldsymbol{u}^{(2)}) \wedge (\boldsymbol{v}^{(1)} = \boldsymbol{v}^{(2)})\right) \wedge$$
$$\left((\boldsymbol{c}^{(2)} = \boldsymbol{c}^{(1)} + 1) \to (\boldsymbol{v}^{(1)} = \boldsymbol{u}^{(2)})\right) \wedge$$
$$\left((\boldsymbol{c}^{(1)} = 0) \to S(\boldsymbol{u}^{(1)})\right) \wedge \left((\boldsymbol{c}^{(1)} = 2^k - 1) \to T(\boldsymbol{v}^{(1)})\right) \wedge \delta\left(\boldsymbol{u}^{(1)}, \boldsymbol{v}^{(1)}\right)$$

Comparison with QBF encodings:

DQBF needs only $O(n)$ existential variables vs. $O(k \cdot n)$.

DQBF Encodings 6/6

- QBF: two-player game, 1 univ. vs 1 ex. player, PSPACE-complete
- DQBF: three-player game, 1 univ vs 2 ex. players, NEXPTIME-complete (⟶ MIP [Babai et al. 1991])

  Dependencies make sure that the existential players do not communicate.

  Allows encodings which reuse space.

  Example: create unique existentials indexed by $\boldsymbol{i}$

  $\forall \boldsymbol{i} \forall \boldsymbol{i}' \exists \boldsymbol{y}(\boldsymbol{i}) \exists \boldsymbol{y}(\boldsymbol{i}') \left((\boldsymbol{i} = \boldsymbol{i}') \rightarrow (\boldsymbol{y} = \boldsymbol{y}')\right) \land \left((\boldsymbol{i} \neq \boldsymbol{i}') \rightarrow (\boldsymbol{y} \neq \boldsymbol{y}')\right)$

DQBF Reasoning Techniques

Important techniques for QBF:

- Q-resolution

  open problem for DQBF

- Universal quantifier expansion

  $$\forall x \exists y\, \Phi(x, y) \approx \exists y_0 \exists y_1\, \Phi(0, y_0) \wedge \Phi(1, y_1)$$

  For QBF, expansion follows immediately from the inductive QBF semantics.

  A generalization to the function semantics of DQBF can be proven.

DQBF Universal Expansion

Theorem [Bubeck, 2010]

$$\forall x_1 \ldots \forall x_n \exists y_1(\boldsymbol{x}_{\boldsymbol{d}_1}) \ldots \exists y_k(\boldsymbol{x}_{\boldsymbol{d}_k})$$
$$\exists y_{k+1}(\boldsymbol{x}_{\boldsymbol{d}_{k+1}}, x_n) \ldots \exists y_m(\boldsymbol{x}_{\boldsymbol{d}_m}, x_n)$$
$$\phi(x_1, \ldots, x_n, y_1, \ldots, y_m, \boldsymbol{z})$$

with $x_n \notin \boldsymbol{x}_{\boldsymbol{d}_i}$ for $i \leq k$

is equivalent to

$$\forall x_1 \ldots \forall x_{n-1} \cancel{\forall x_n} \exists y_1(\boldsymbol{x}_{\boldsymbol{d}_1}) \ldots \exists y_k(\boldsymbol{x}_{\boldsymbol{d}_k})$$
$$\exists y_{k+1,(0)}, y_{k+1,(1)}(\boldsymbol{x}_{\boldsymbol{d}_{k+1}} \cancel{, x_n}) \ldots \exists y_{m,(0)}, y_{m,(1)}(\boldsymbol{x}_{\boldsymbol{d}_m} \cancel{, x_n})$$
$$\phi(x_1, \ldots, x_{n-1}, 0, y_1, \ldots, y_k, y_{k+1,(0)}, \ldots, y_{m,(0)}, \boldsymbol{z}) \wedge$$
$$\phi(x_1, \ldots, x_{n-1}, 1, y_1, \ldots, y_k, y_{k+1,(1)}, \ldots, y_{m,(1)}, \boldsymbol{z}).$$

DQBF Subclasses

Whole Matrix Restrictions 1/2

Known tractable subclasses:

- DQ2-CNF satisfiability is solvable in linear time by a modification of the Aspvall / Plass / Tarjan algorithm.

  [Bubeck / Kleine Büning, 2010]

- DQHORN satisfiability is solvable in quadratic time.

  [Bubeck / Kleine Büning, 2006]

Whole Matrix Restrictions 2/2

Modification of the Aspvall / Plass / Tarjan algorithm:

- Q2-CNF unsatisfiability criterion (2):
  a universal node over x is in the same strongly connected component as an existential node over y and $\exists y$ precedes $\forall x$ in the prefix.
- DQ2-CNF unsatisfiability criterion (2'):
  a universal node over x is in the same strongly connected component as an existential node over y and y does not depend on x.

Generalized HORN 1/3

For DQCNF formulas with free variables, we split each clause ϕ_i into a bound part $\phi_i^b(v_1, \ldots, v_n)$ and a free part $\phi_i^f(z_1, \ldots, z_r)$ (both may be empty):

$$\Phi(z_1, \ldots, z_r) = Q_1 v_1 \ldots Q_n v_n \wedge_i \left(\phi_i^b(v_1, \ldots, v_n) \vee \phi_i^f(z_1, \ldots, z_r)\right)$$

Then DQHORN^b is the subclass of DQCNF formulas with free variables where

- $Q_1 v_1 \ldots Q_n v_n \ \wedge_i \phi_i^b(v_1, \ldots, v_n)$ is a formula in DQHORN, and
- each $\phi_i^f(z_1, \ldots, z_r)$ is an arbitrary clause over free variables.

Generalized HORN 2/3

For every $\Phi \in$ DQHORN^b with $|\forall|$ universal quantifiers, there exists a logically equivalent $\exists$HORN^b formula of quadratic length $O(|\forall| \cdot |\Phi|)$

which can be computed also in time $O(|\forall| \cdot |\Phi|)$.

[Bubeck, 2010]

That means DQHORN^b satisfiability is NP-complete.

Similarly, a transformation in time $O(|\forall|^2 \cdot |\Phi|)$ is possible from DQ2-CNF^b to $\exists$2-CNF^b.

[Bubeck / Kleine Büning, 2010]

Generalized HORN 3/3

Idea for the DQHORN^b to $\exists$HORN^b transformation:

Model functions for closed DQHORN can be written as intersection of individual assignments for cases with at most one universal being zero.

$$
\begin{aligned}
f^t_{y_i}(x_{d_{i,1}}, \ldots, x_{d_{i,n_i}}) \quad := \quad & (\neg x_{d_{i,1}} \rightarrow \boxed{f_{y_i}(0,1,1,\ldots,1)}) \\
\wedge \quad & (\neg x_{d_{i,2}} \rightarrow \boxed{f_{y_i}(1,0,1,\ldots,1)}) \\
\wedge \quad & \ldots \\
\wedge \quad & (\neg x_{d_{i,n_i}} \rightarrow \boxed{f_{y_i}(1,1,\ldots,1,0)}) \\
\wedge \quad & \boxed{f_{y_i}(1,\ldots,1)}
\end{aligned}
$$

We only need to know these values
$\rightarrow$ partial model

This allows a simultaneous expansion of all universals with at most one universal being zero in each copy.

Section 5

Conclusion

Conclusion

- DQBF corresponds to three-player games with 1 universal versus 2 existential players. Dependencies make sure that the existential players do not communicate.
- DQBF allows encodings which can reuse space.
- Dependency quantification seems significantly less powerful under CNF matrices with further restrictions (HORN, 2-CNF), even if the restrictions apply only to bound variables.

Open Questions

- Universal expansion can be generalized to DQBF.
  What about Q-resolution for DQBF?
- Are there other interesting DQBF subclasses?
- How to solve DQBF in practice?

The End