Dependency Quantified Boolean Formulas

Uwe Bubeck
Universität Paderborn

17.01.2013
Outline

• Introduction
• Models
• Dependency Quantification
• DQBF Subclasses
• Conclusion
Introduction
QBF extends propositional logic by allowing universal and existential quantifiers over propositional variables.

**Inductive definition:**

1. Every propositional formula is a QBF.

2. If $\Phi$ is a QBF then $\forall x \Phi$ and $\exists y \Phi$ are also QBFs.

3. If $\Phi_1$ and $\Phi_2$ are QBFs then $\neg \Phi_1$, $\Phi_1 \land \Phi_2$ and $\Phi_1 \lor \Phi_2$ are also QBFs.
In a closed QBF, every variable is quantified.

**Semantics definition for closed QBF:**

\[ \exists y \Phi(y) \text{ is true if and only if } \Phi[y/0] \text{ is true or } \Phi[y/1] \text{ is true.} \]

\[ \forall x \Phi(x) \text{ is true if and only if } \Phi[x/0] \text{ is true and } \Phi[x/1] \text{ is true.} \]

A closed QBF is either true or false.
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 $t \in T$?
In Bounded Model Checking, vertices are typically binary vectors \((V = \{0,1\}^n)\), and the edges are given by a transition relation \(\delta\):

\[\delta(u, v) = 1 \text{ iff there is an edge from } u = (u_1, \ldots, u_n) \text{ to } v = (v_1, \ldots, v_n).\]

If \(\delta\) is encoded as a propositional formula, the whole reachability test can be formulated in propositional logic:

\[
S(v_0) \land T(v_{2^k}) \bigwedge_{i=0}^{2^k - 1} \delta(v_i, v_{i+1})
\]
Problem: many copies of $\delta$

Compress conjunctions of renamings / instantiations by universal variables:

$$S(v_0) \land T(v_2^k) \land \forall u \forall w \left( \left( \bigvee_{i=0}^{2^k-1} ((u = v_i) \land (w = v_{i+1})) \right) \rightarrow \delta(u, w) \right)$$

[Dershowitz et al., 2005], [Meyer/Stockmeyer, 1973]
Even more compact: 

\[
\begin{align*}
\delta_{2k}(a, b) &{} := \exists z \ \delta_{2k-1}(a, z) \land \delta_{2k-1}(z, b) \\
\vdots \\
\delta_1(a, b) &{} := \delta(a, b)
\end{align*}
\]
Even more compact: iterative squaring

\[ \nu_0 \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu_{2^k} \]

\[ \nu_0 \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu \rightarrow \nu_{2^k} \]

\[ \exists z \forall u \forall w \left( (u = a) \land (w = z) \right) \lor \left( (u = z) \land (w = b) \right) \rightarrow \delta_{2^{k-1}}(u, w) \]

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

[Meyer/Stockmeyer, 1973]
Models
\[ \forall x_1 \exists y_1 \forall x_2 \exists y_2 \ (x_1 \lor \neg y_1) \land (\neg x_1 \lor y_2) \land (y_1 \lor x_2 \lor \neg y_2) \land (\neg x_2 \lor y_2) \]
∀\(x_1 \exists y_1 \exists y_2 \ (x_1 \lor \neg y_1) \land (\neg x_1 \lor y_2) \land (y_1 \lor x_2 \lor \neg y_2) \land (\neg x_2 \lor y_2)\)
∀x₁ ∃y₁ ∀x₂ ∃y₂ (x₁ ∨ ¬y₁) ∧ (¬x₁ ∨ y₂) ∧ (y₁ ∨ x₂ ∨ ¬y₂) ∧ (¬x₂ ∨ y₂)
∀x₁ ∃y₁ ∀x₂ ∃y₂ \( (x_1 \lor \neg y_1) \land (\neg x_1 \lor y_2) \land (y_1 \lor x_2 \lor \neg y_2) \land (\neg x_2 \lor y_2) \)

Uwe Bubeck

Dependency Quantified Boolean Formulas
15
∀\(x_1\exists y_1 \forall x_2 \exists y_2\) \((x_1 \lor \neg y_1) \land (\neg x_1 \lor y_2) \land (y_1 \lor x_2 \lor \neg y_2) \land (\neg x_2 \lor y_2)\)

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

A closed prenex QBF $\Phi$ with existential variables $y_1, \ldots, y_m$ is true iff there exist $f_{y_1}, \ldots, f_{y_m}$ 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 $\Phi[y_1/f_{y_1}, \ldots, y_m/f_{y_m}]$ of all variable occurrences with corresponding functions produces a true formula.
Dependency Quantification
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 $\{x_1\} \not\subseteq \{x_2\}$. 
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 \( \phi \) is a propositional matrix over \( x_1, \ldots, x_n, y_1, \ldots, y_m \).

**Semantics Definition**

\( \Phi \) 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.
Generalization to DQBF with free variables [Bubeck, 2010]

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

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

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

Semantics Definition

$\Phi \in$ DQBF with free variables $z_1, ..., z_r$ is satisfiable iff there exists a truth assignment $(\tau(z_1), ..., \tau(z_r)) \in \{0,1\}^r$ such that $\Phi[z_1/\tau(z_1), ..., z_r/\tau(z_r)]$ is true.
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 $\exists y_i(x_{d_i,1}, \ldots, x_{d_i,n_i})$ in DPLL style, add a **Skolem clause** $(l(x_{d_i,1}) \land \cdots \land l(x_{d_i,n_i})) \rightarrow l(y_i)$

where $l(\nu) = \nu$ or $l(\nu) = \neg \nu$ according to the current assignment to $\nu$. 
Theorem

The DQBF satisfiability problem is NEXPTIME-complete.

[Peterson / Reif, 1979]

This even holds for relatively simple prefixes of the form

\[ \forall u \forall v \exists y (u) \exists z (v) \]

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

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

\[
(\forall u \exists y \phi(u, y)) \land (\forall v \exists z \psi(v, z))
\]

\[ \approx \forall u \forall v \exists y \exists z (\phi(u, y) \land \psi(v, z)) \]
Additional restriction of non-prenex QBF: variables from disjoint quantifier scopes cannot occur in common subformulas:

\[(\forall u \exists y \phi(u, y)) \land (\forall v \exists z \psi(v, z) \land \tau(y, z))\]

not possible

Why combine „unrelated“ variables in one subformula?
Alternative modeling approach for bounded reachability:

Two-player game where

- universal player presents a step counter \( c = (c_1, \ldots, c_k) \),
- existential player must find corresponding \( u \) and \( v \)

so that \((c = 0) \rightarrow S(u)\), \((c = 2^k - 1) \rightarrow T(v)\) and \( \delta(u, v) \).

QBF formulation:

\[
\forall c \exists u \exists v ((c = 0) \rightarrow S(u)) \land ((c = 2^k - 1) \rightarrow T(v)) \land \delta(u, v)
\]

→ Clearly flawed: does not enforce a continuous path.
Use two existential players and two counters:

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

\[
\forall c^{(1)} \exists u^{(1)} \exists v^{(1)} \forall c^{(2)} \exists u^{(2)} \exists v^{(2)} \\
((c^{(2)} = c^{(1)}) \rightarrow (u^{(1)} = u^{(2)}) \land (v^{(1)} = v^{(2)})) \land \\
((c^{(2)} = c^{(1)} + 1) \rightarrow (v^{(1)} = u^{(2)})) \land \\
((c^{(1)} = 0) \rightarrow S(u^{(1)})) \land ((c^{(1)} = 2^k - 1) \rightarrow T(v^{(1)})) \land \delta(u^{(1)}, v^{(1)})
\]
∀ 𝒄^{(1)} ∃ 𝒉^{(1)} ∃ 𝒗^{(1)} ∀ 𝒄^{(2)} ∃ 𝒉^{(2)} ∃ 𝒗^{(2)}

\((\left( 𝒄^{(2)} = 𝒄^{(1)} \right) \rightarrow (ℎ^{(1)} = ℎ^{(2)}) \land (𝒗^{(1)} = 𝒗^{(2)}))\) ∧

\((\left( 𝒄^{(2)} = 𝒄^{(1)} + 1 \right) \rightarrow (𝒗^{(1)} = ℎ^{(2)}))\) ∧

\((\left( 𝒄^{(1)} = 0 \right) \rightarrow S(ℎ^{(1)})) \land (\left( 𝒄^{(1)} = 2^k - 1 \right) \rightarrow T(𝒗^{(1)}))\) ∧ δ(ℎ^{(1)}, 𝒗^{(1)})

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

\(𝒄^{(1)} = τ, 𝒄^{(2)} = τ + 1: \) \hspace{1cm} \(𝒄^{(1)} = τ + 1, 𝒄^{(2)} = τ + 1: \)

Player 1: \(a \rightarrow b\) \hspace{1cm} Player 1: \(d \rightarrow e\)

Player 2: \(b \rightarrow c\) \hspace{1cm} Player 2: \(b \rightarrow c \hspace{1cm} d \rightarrow e\)
Choice of $u^{(2)}$ and $v^{(2)}$ should only depend on $c^{(2)}$.

Solution: *explicitly indicate dependencies* in DQBF

\[
\forall c^{(1)} \forall c^{(2)} \exists u^{(1)}(c^{(1)}) \exists v^{(1)}(c^{(1)}) \exists u^{(2)}(c^{(2)}) \exists v^{(2)}(c^{(2)})
\]

\[
((c^{(2)} = c^{(1)}) \rightarrow (u^{(1)} = u^{(2)}) \land (v^{(1)} = v^{(2)))) \land
\]

\[
((c^{(2)} = c^{(1)} + 1) \rightarrow (v^{(1)} = u^{(2)})) \land
\]

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

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 $i$

$$\forall i \forall i' \exists y(i) \exists y(i') \left( (i = i') \rightarrow (y = y') \right) \land \left( (i \neq i') \rightarrow (y \neq y') \right)$$
Important techniques for QBF:

- **Q-resolution**
  
  open problem for DQBF

- **Universal quantifier expansion**

  \[ \forall x \exists y \Phi(x, y) \approx \exists y_0 \exists y_1 \Phi(0, y_0) \land \Phi(1, y_1) \]

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

  A generalization to the function semantics of DQBF can be proven.
Theorem [Bubeck, 2010]

\[ \forall x_1 \ldots \forall x_n \exists y_1(x_{d_1}) \ldots \exists y_k(x_{d_k}) \]
\[ \exists y_{k+1}(x_{d_{k+1}}, x_n) \ldots \exists y_m(x_{d_m}, x_n) \]
\[ \phi(x_1, \ldots, x_n, y_1, \ldots, y_m, z) \]

with \( x_n \notin x_{d_i} \) for \( i \leq k \)

is equivalent to

\[ \forall x_1 \ldots \forall x_{n-1} \forall x_{\overline{n}} \exists y_1(x_{d_1}) \ldots \exists y_k(x_{d_k}) \]
\[ \exists y_{k+1}(0), y_{k+1}(1)(x_{d_{k+1}}, x_{\overline{n}}) \ldots \exists y_m(0), y_m(1)(x_{d_m}, x_{\overline{n}}) \]
\[ \phi(x_1, \ldots, x_{n-1}, 0, y_1, \ldots, y_k, y_{k+1}(0), \ldots, y_m(0), z) \land \]
\[ \phi(x_1, \ldots, x_{n-1}, 1, y_1, \ldots, y_k, y_{k+1}(1), \ldots, y_m(1), z). \]
DQBF Subclasses
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 $x$.
For DQCNF formulas with free variables, we split each clause $\phi_i$ 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):

$$\Phi(z_1, \ldots, z_r) = Q_1 v_1 \ldots Q_n v_n \land_i (\phi_i^b(v_1, \ldots, v_n) \lor \phi_i^f(z_1, \ldots, z_r))$$

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

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

$$f_{y_i}^t(x_{d_i,1}, \ldots, x_{d_i,n_i}) := \neg x_{d_i,1} \rightarrow f_{y_i}(0, 1, 1, \ldots, 1)$$
$$\wedge (\neg x_{d_i,2} \rightarrow f_{y_i}(1, 0, 1, \ldots, 1))$$
$$\wedge \ldots$$
$$\wedge (\neg x_{d_i,n_i} \rightarrow f_{y_i}(1, 1, \ldots, 1, 0))$$
$$\wedge f_{y_i}(1, \ldots, 1)$$

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.
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 \textit{Q-resolution for DQBF}?

• Are there other interesting \textit{DQBF subclasses}?

• How to solve \textit{DQBF in practice}?
The End