CURRENT TRENDS IN QBF SOLVING

Mikoláš Janota

BNP 2016, Phoenix AZ

Microsoft Research, Cambridge, UK

- SAT — for a Boolean formula, determine if it is satisfiable
- Example: $(x \vee y) \wedge (x \vee \neg y)$
  $x \triangleq 1, y \triangleq 0$
- QBF — for a *Quantified* Boolean formula, determine if it is true
- Example: $\forall x \exists y.\ (x \leftrightarrow y)$
- Quantifications as shorthands for connectives ($\forall = \wedge, \exists = \vee$)

  Example:
  1. $\forall x \exists y.\ (x \leftrightarrow y)$
  2. $\forall x.\ (x \leftrightarrow 0) \vee (x \leftrightarrow 1)$
  3. $((0 \leftrightarrow 0) \vee (0 \leftrightarrow 1)) \wedge ((1 \leftrightarrow 0) \vee (1 \leftrightarrow 1))$
  4. 1 (True)

RELATION TO COMPLEXITY THEORY

$$
\begin{tikzcd}[column sep=small]
\vdots & \vdots & & & \vdots & \vdots \\
\forall Z \exists Y \forall X.\, \phi & \Pi_3^P & & & \Sigma_3^P & \exists Z \forall Y \exists X.\, \phi \\
\forall Y \exists X.\, \phi & \Pi_2^P \arrow[u] & & & \Sigma_2^P \arrow[u] & \exists Y \forall X.\, \phi \\
\forall X.\, \phi & \Pi_1^P = \text{co-NP} \arrow[u] & & & \Sigma_1^P = \text{NP} \arrow[u] & \exists X.\, \phi \\
& & & \text{P} \arrow[ull] \arrow[ur] & &
\end{tikzcd}
$$

- Deciding QBF is PSPACE complete

RELATION TO TWO-PLAYER GAMES

- In this talk we consider prenex form:
  Quantifier-prefix. *Matrix*
  Example $\forall y_1 y_2 \exists x_1 x_2 . (\neg y_1 \vee x_1) \wedge (y_2 \vee \neg x_2)$
- A QBF represents a two-player games between $\forall$ and $\exists$.
- $\forall$ wins a game if the matrix becomes false.
- $\exists$ wins a game if the matrix becomes true.
- A QBF is false iff there exists a winning strategy for $\forall$.
- A QBF is true iff there exists a winning strategy for $\exists$.
  Example

$$\forall u \exists e . (u \leftrightarrow e)$$

$\exists$-player wins by playing $e \triangleq u$.

WHY QUANTIFIED BOOLEAN FORMULAS?

- “Funamental problem”: PSPACE, 2-player games (fin. space)
- Direct applications
    - model checking (subproblems)
    - (circuit) synthesis
    - non-monotonic reasoning
    - conformant planning
    - ...
- In other reasoners?
    - SMT (e.g. Quantified bit vectors)
    - optimization with quantification (“MaxQBF”)
    - ...

Given a CNF ϕ, construct the following QBF.

$$\exists S \forall X. \neg \left(\bigwedge_{C \in \phi} (\neg s_C \vee C) \right) \wedge |S| \leq k$$

Where

- $S = \{s_C \mid C \in \phi\}$ are fresh variables
- X are the original variables of ϕ
- $k \in \mathbb{N}$

[Ignatiev et al., 2015]

PROPAGATION IN QCNF

CDCL SAT solving can be lifted to QBF [Zhang and Malik, 2002].

Example $\exists$-propagation:

$$\forall x_1 \exists x_2 \ldots \forall x_k \exists x_{k+1} \ldots . \; (x_1 \vee x_2 \vee x_k \vee x_{k+1}) \wedge \phi$$

- If $x_1 = x_{k+1} = 0$, then $\exists$ must play $x_2 = 1$.
- As otherwise $\forall$ would win by setting $x_k = 0$.

Example $\forall$-propagation:

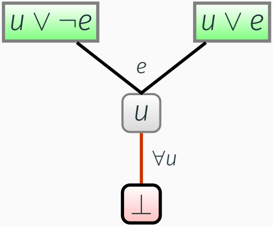
$$\exists x_1 \ldots \forall x_k \ldots . \; (x_k \vee C_1) \wedge (x_k \vee C_2) \wedge (x_1 \vee C_3)$$

- If $x_1 = 1$, then $\forall$ must play $x_k = 0$.

Unification for the 2 players: [Zhang, 2006] [Klieber, 2014] [Goultiaeva et al., 2013]

Q-resolution=Q-resolution rule + $\forall$-reduction [Büning et al., 1995]

$$\forall u \exists e. \, (u \vee \neg e) \wedge (u \vee e)$$

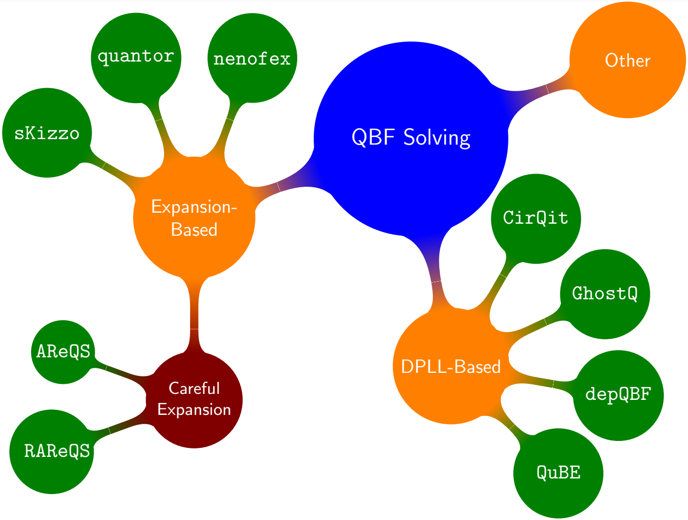


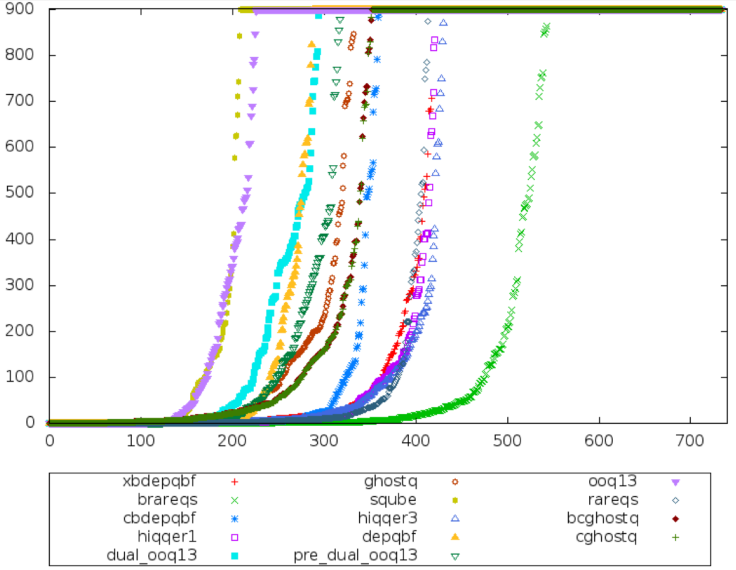
$$\exists \mathcal{E}\, \forall \mathcal{U}.\, \phi = \exists \mathcal{E}.\, \bigwedge_{\mu \in 2^{\mathcal{U}}} \phi[\mu]$$

Can be solved by SAT $\left(\bigwedge_{\mu \in 2^{\mathcal{U}}} \phi[\mu]\right)$. Impractical!

Expand gradually instead: [Janota et al., 2012]

- Pick τ_0 arbitrary assignment to $\mathcal{E}$
- $\mathsf{SAT}(\neg\phi[\tau_0]) = \mu_0$ assignment to $\mathcal{U}$
- $\mathsf{SAT}(\phi[\mu_0]) = \tau_1$ assignment to $\mathcal{E}$
- $\mathsf{SAT}(\neg\phi[\tau_1]) = \mu_2$ assignment to $\mathcal{U}$
- $\mathsf{SAT}(\phi[\mu_0] \wedge \phi[\mu_1]) = \tau_2$ assignment to $\mathcal{E}$

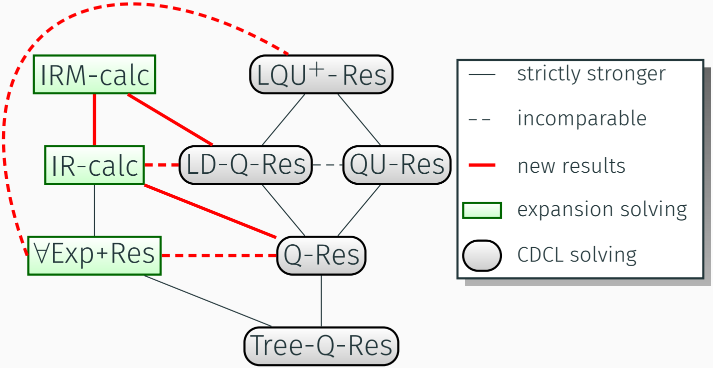

QBF Solving
Other
Expansion-Based
quantor
nenofex
sKizzo
Careful Expansion
AReQS
RAReQS
DPLL-Based
CirQit
GhostQ
depQBF
QuBE


900
800
700
600
500
400
300
200
100
0
0
100
200
300
400
500
600
700
xbdepqbf
brareqs
cbdepqbf
hiqqer1
dual_ooq13
ghostq
sqube
hiqqer3
depqbf
pre_dual_ooq13
ooq13
rareqs
bcghostq
cghostq

WHAT ABOUT THEORY?

- CDCL is characterized by Q-resolution [Büning et al., 1995]
- Expansion is characterized by ∀Exp+Res [Janota and Marques-Silva, 2015]
- These calculi are incomparable [Beyersdorff et al., 2015].

CALCULI ZOO [Beyersdorff et al., 2015]



SUMMARY AND CHALLENGES

- There are two distinct approaches to solving: expansion and conflict-driven learning
- The approaches correspond to different proof systems, which are incomparable.
- Challenge: There are calculi with no corresponding solvers.
- Challenge: There are formula with easy strategies but that are hard to solve. How to look for strategies? [Bjørner et al., 2015]
- Challenge: How to make QBF more attractive, more theories? [Bjørner and Janota, 2015]

Beyersdorff, O., Chew, L., and Janota, M. (2015).
Proof complexity of resolution-based QBF calculi.
In *STACS*.

Bjørner, N. and Janota, M. (2015).
Playing with quantified satisfaction.
In *LPAR*.

Bjørner, N., Janota, M., and Klieber, W. (2015).
On conflicts and strategies in QBF.
In *LPAR*.

Büning, H. K., Karpinski, M., and Flögel, A. (1995).
Resolution for quantified Boolean formulas.
Inf. Comput., 117(1).

Goultiaeva, A., Seidl, M., and Biere, A. (2013).
Bridging the gap between dual propagation and CNF-based QBF solving.

In *DATE*, pages 811–814.

Ignatiev, A., Janota, M., and Marques-Silva, J. (2015).
Quantified maximum satisfiability.
Constraints, pages 1–26.

Janota, M., Klieber, W., Marques-Silva, J., and Clarke, E. M. (2012).
Solving QBF with counterexample guided refinement.
In *SAT*, pages 114–128.

Janota, M. and Marques-Silva, J. (2015).
Expansion-based QBF solving versus Q-resolution.
Theoretical Computer Science, 577(0):25–42.

Klieber, W. (2014).
Formal Verification Using Quantified Boolean Formulas (QBF).
PhD thesis, Carnegie Mellon University.

Zhang, L. (2006).
Solving QBF by combining conjunctive and disjunctive normal forms.
In *AAAI*.

Zhang, L. and Malik, S. (2002).
Conflict driven learning in a quantified Boolean satisfiability solver.
In *ICCAD*.