Q-Resolution with Generalized Axioms

Florian Lonsing[1] Uwe Egly[1] Martina Seidl[2]

[1]Knowledge-Based Systems Group, Vienna University of Technology, Austria

[2]Institute for Formal Models and Verification, JKU Linz, Austria

19th International Conference on Theory and Applications of Satisfiability Testing, 5 - 8 July 2016, Bordeaux, France

This work is supported by the Austrian Science Fund (FWF) under grants S11408-N23 and S11409-N23.

Introduction (1/4)

Q-Resolution Calculus (QRES): [KBKF95]

- Prenex CNF $\psi = \hat{Q}.\phi$ unsatisfiable iff empty clause derivable from ψ.
- Completeness: resolution on $\exists$ pivots and universal reduction.
- Resolution on $\forall$ pivots (QU-resolution) [VG12], long-distance resolution [ZM02a, BJ12], combinations thereof [BWJ14].
- QRES-based calculi vs. expansion/instantiation [BCJ15, JM15].
- Traditional QRES used for clause learning in QCDCL.

Introduction (1/4)

Problem:

- Problem (cf. previous talk [Jan16]): current implementations of QCDCL do not harness the full power of QRES in clause learning.
- Resolution in QCDCL guided by assignments.
- Prefix ordering restricts assignment generation in QCDCL.
- Axioms of QRES are weak.

Introduction (2/4): QRES Clause Derivations

Definition (Clause Axiom of QRES)

$$\frac{}{C}$$ Given a PCNF $\psi = \hat{Q}.\phi$, $C \in \phi$ and for all $x \in \hat{Q}$: $\{x, \bar{x}\} \not\subseteq C$.

Example

- Traditional Q-resolution [KBKF95].
- Only $\exists$ pivots.
- No tautologies.

$$\dfrac{(x) \qquad \dfrac{\dfrac{(\bar{x} \vee u \vee y) \qquad (\bar{x} \vee u \vee \bar{y})}{(\bar{x} \vee u)}}{(\bar{x})}}{\emptyset}$$

$\psi = \exists x \forall u \exists y \forall v \exists z.$
$(x) \wedge$
$(\bar{x} \vee u \vee y) \wedge$
$(\bar{x} \vee u \vee \bar{y}) \wedge$
$(x \vee \bar{u} \vee \bar{z})$
$(x \vee u \vee \bar{z})$

- QRES variants: different power but same clause axiom.
- Clause axiom derives only input clauses (falsified in QCDCL).

Introduction (2/4): QRES Clause Derivations

Definition (Clause Axiom of QRES)

$$\frac{}{C} \qquad \text{Given a PCNF } \psi = \hat{Q}.\phi,\ C \in \phi \text{ and for all } x \in \hat{Q}\text{: } \{x, \bar{x}\} \not\subseteq C.$$

Example

- Long distance Q-resolution [ZM02a, BJ12].
- Only $\exists$ pivots.
- Tautologies over $\forall$ variables (pivot level!).

$$\dfrac{(\bar{x} \vee u \vee \bar{y}) \qquad (x \vee \bar{u} \vee \bar{z})}{(u \vee \bar{u} \vee \bar{y} \vee \bar{z})}$$

$$\begin{aligned}\psi = \exists x \forall u \exists y \forall v \exists z.\ & (x) \wedge \\ & (\bar{x} \vee u \vee y) \wedge \\ & (\bar{x} \vee u \vee \bar{y}) \wedge \\ & (x \vee \bar{u} \vee \bar{z}) \\ & (x \vee u \vee \bar{z})\end{aligned}$$

- QRES variants: different power but same clause axiom.
- Clause axiom derives only input clauses (falsified in QCDCL).

Introduction (2/4): QRES Clause Derivations

Definition (Clause Axiom of QRES)

$$\overline{C}$$ Given a PCNF $\psi = \hat{Q}.\phi$, $C \in \phi$ and for all $x \in \hat{Q}$: $\{x, \bar{x}\} \not\subseteq C$.

Example

- QU-resolution [VG12].
- $\forall/\exists$ pivots.
- No tautologies.
- LQU^{+}-Res: $\forall/\exists$ pivots and tautologies [BWJ14].

$$\frac{(x \vee \bar{u} \vee \bar{z}) \quad (x \vee u \vee \bar{z})}{(x \vee \bar{z})}$$

$$\psi = \exists x \forall u \exists y \forall v \exists z. \\ (x) \wedge \\ (\bar{x} \vee u \vee y) \wedge \\ (\bar{x} \vee u \vee \bar{y}) \wedge \\ (x \vee \bar{u} \vee \bar{z}) \\ (x \vee u \vee \bar{z})$$

- QRES variants: different power but same clause axiom.
- Clause axiom derives only input clauses (falsified in QCDCL).

Introduction (3/4)

QRES for Satisfiable QBFs: [GNT06, Let02, ZM02b]

- Operates on cubes (conjunctions of literals).
- Dual to QRES for clauses: cube resolution and existential reduction.
- Prenex CNF $\psi = \hat{Q}.\phi$ satisfiable iff empty cube derivable from ψ.
- Traditional QRES used for cube learning in QCDCL.

Introduction (4/4): QRES Cube Derivations

Definition (Cube Axiom of QRES [GNT06, Let02, ZM02b])

$$\frac{}{C}$$

Given a PCNF $\psi = \hat{Q}.\phi$ and an assignment A with $\{x, \bar{x}\} \not\subseteq A$ and $\psi[A] = \top$, $C = (\bigwedge_{l \in A})$ is a cube.

Example

- Axiom: model generation.
- Cubes at leaves are part of DNF of ϕ.
- Existential reduction.
- Cube resolution.

$$\dfrac{\dfrac{\dfrac{(\bar{x} \wedge u \wedge \bar{y})}{(\bar{x} \wedge u)} \qquad \dfrac{(\bar{x} \wedge \bar{u} \wedge y)}{(\bar{x} \wedge \bar{u})}}{(\bar{x})}}{\emptyset}$$

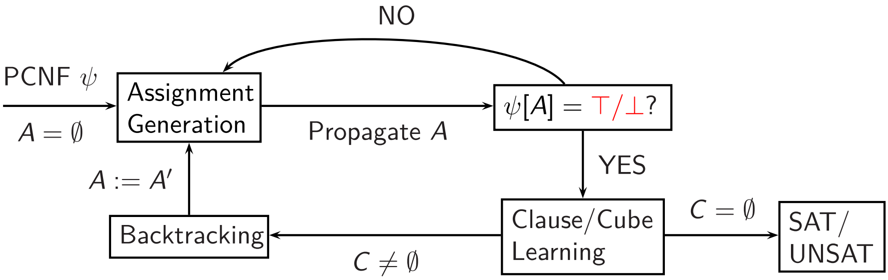
$\psi = \exists x \forall u \exists y.$
$(\bar{x} \vee u \vee \bar{y}) \wedge$
$(\bar{x} \vee \bar{u} \vee y) \wedge$
$(x \vee u \vee y) \wedge$
$(x \vee \bar{u} \vee \bar{y})$

- Cube axiom allows to derive only CNF models of ψ.
- Trivial formulas with exponential cube proofs: [RBM97, Let02]
  $\Psi(n) = \forall u_1 \exists x_1 \ldots \forall u_n \exists x_n. \bigwedge_{i=1}^{n} \left[(u_i \vee \bar{x}_i) \wedge (\bar{u}_i \vee x_i)\right]$

Contributions

- Generalized axioms: stronger clauses/cubes at leaves of derivations.
- Idea: check satisfiability of PCNF ψ under assignment A in QCDCL.
- Integration of arbitrary QBF proof system in QRES via axioms.
- Stronger QRES variants by integrating orthogonal proof systems.
- Tight integration in QCDCL by learning asserting clauses/cubes.
- Implementation in DepQBF, experimental study.
- Formula class CR_n from previous talk [Jan16]: short QRES proofs by QCDCL based on stronger axiom.

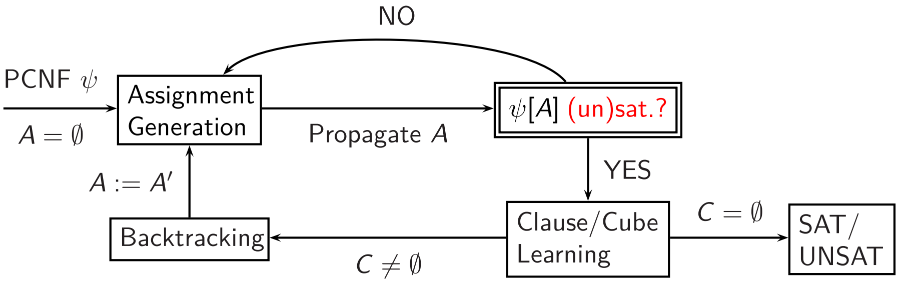
QCDCL (1/2)



Traditional Axioms:

- *QCDCL assignments*: select decision variables from left end of prefix of $\psi[A]$, unit and pure literal detection out of prefix order.
- $\psi[A] = \bot$: CNF ϕ contains a falsified clause.
- $\psi[A] = \top$: all clauses in CNF ϕ satisfied.
- Asserting clause (cube) C: $C[A']$ unit for some $A' \subseteq A$.

QCDCL (2/2)



Generalized Axioms:

- Check satisfiability of $\psi[A]$ in QBCP by incomplete approaches.
- QBF is hard: spend more time on reasoning before assigning decision variables (similar argument as in, e.g., [SB06]).
- $\psi[A]$ (un)sat.: derive asserting clause (cube) C from a start clause (cube) generated based on A.

Generalized Axioms: Theory

Definition (Generalized Clause Axiom)

$$\frac{}{C}$$

Given a PCNF $\psi = \hat{Q}.\phi$ and a QCDCL assignment A, $\psi[A]$ is unsatisfiable, and $C = (\bigvee_{l \in A} \overline{l})$ is a clause.

Definition (Generalized Cube Axiom)

$$\frac{}{C}$$

Given a PCNF $\psi = \hat{Q}.\phi$ and a QCDCL assignment A, $\psi[A]$ is satisfiable, and $C = (\bigwedge_{l \in A} l)$ is a cube.

Proposition (Soundness)

For a clause (cube) C derived by the generalized clause (cube) axiom: $\hat{Q}.\phi \equiv_{sat} \hat{Q}.(\phi \wedge C)$, respectively $\hat{Q}.\phi \equiv_{sat} \hat{Q}.(\phi \vee C)$.

Generalized Axioms: Practice

Axiom Applications in QCDCL:

- *Any* QBF proof system can be used to check satisfiability of $\psi[A]$.
- Combinations of proof systems within QRES via generalized axioms.
- Clauses (cubes) by generalized axioms used as usual in learning.
- Checking satisfiability of PCNF $\psi[A]$ is PSPACE-complete.

Incomplete QBF Satisfiability Checks:

- E.g. bounded variable expansion [Bie04, BB07]: QBF preprocessing.
- E.g. SAT-based techniques in early QDPLL [CGS98]:
  - Trivial truth: check ψ' obtained by discarding all $\forall$ literals in ψ.
  - Trivial falsity: check ψ' obtained by treating every variable in ψ as $\exists$.
- If unsuccessful: extend A to A' by decisions and QBCP, check $\psi[A']$.

Formalizing the Use of SAT Solving

Definition (Abstraction-Based Clause Axiom)

For PCNF $\psi = \hat{Q}.\phi$, $Abs_{\exists}(\psi) := \exists(X_1 \cup \ldots \cup X_n).\phi$.

$$\frac{}{C} \quad \text{For a PCNF } \psi = \hat{Q}.\phi \text{, and a (non-)QCDCL assignment } A\text{, } Abs_{\exists}(\psi)[A] \text{ is unsatisfiable, and } C = (\bigvee_{l \in A} \bar{l}) \text{ is a clause.}$$

Proposition (cf. appendix of [LES16])

QRES with the abstraction-based clause axiom p-simulates QU-resolution.

Example

$$\frac{C' \cup \{p\} \qquad C'' \cup \{\bar{p}\}}{C' \cup C''}$$

Let $q(p) = \forall$ and clause $C = C' \cup C''$ be derived by QU-resolution.

- For $A = \{\bar{l} \mid l \in C\}$, $Abs_{\exists}(\psi)[A]$ unsatisfiable: $(p), (\bar{p}) \in Abs_{\exists}(\psi)[A]$.
- Hence C derivable by QRES with the abstraction-based clause axiom.

Short Proof of CR_n by QCDCL

Definition ([Jan16])

For $i, j \in \{1, \ldots, n\}$,
$CR_n := \exists x_{ij} \forall z \exists a_i, b_i.(x_{ij} \vee z \vee a_i) \wedge (\bar{x}_{ij} \vee \bar{z} \vee b_j) \wedge (\bigvee \bar{a}_i) \wedge (\bigvee \bar{b}_i)$

1. We assume a "perfect" restart and assignment strategy in QCDCL.
2. By QCDCL, derive $(x_{1,j} \vee \cdots \vee x_{n,j})$ and $(x_{i,1} \vee \cdots \vee x_{i,n})$ for all i, j by QCDCL assignments $A := \{\bar{x}_{1,j} \cdots \bar{x}_{n,j}\}$, $A = \{\bar{x}_{i,1} \cdots \bar{x}_{i,n}\}$.
3. By abstraction-based axiom, derive clauses $(x_{i,j} \vee a_i)$ and $(x_{i,j} \vee b_j)$ by *non-QCDCL* assignments $A := \{\bar{x}_{i,j}, \bar{a}_i\}$ and $A := \{\bar{x}_{i,j}, \bar{b}_j\}$, respectively. (The SAT solver needs the clauses derived in step 2).
4. Derive unit clauses (x_{ij}) in QCDCL using QCDCL assignments $A := \{\bar{x}_{ij}\}$. (By clauses from step 3, we get propagations on a_i, b_i).
5. Get $\emptyset$ by unit resolution with (x_{ij}) clauses, resolution on $(\bigvee \bar{b}_i)$.

All resolution derivations above are polynomial, also inside the SAT solver.

Implementing Generalized Axioms in QCDCL

QBF Preprocessing:

- Incomplete solving.
- QBF preprocessors may have considerable solving power [LSVG16].
- Integration of Bloqqer: `http://fmv.jku.at/bloqqer/`.
- Clause and cube learning wrt. SAT/UNSAT result.
- Nonincremental, $\psi[A]$ added to Bloqqer always from scratch.

Implementing Generalized Axioms in QCDCL

SAT Solving:

- Integration of PicoSAT: abstraction-based axiom, trivial truth.
- Incremental solving under QCDCL assignment A (assumptions).
- Failed assumptions $A' \subseteq A$: already $Abs_{\exists}(\psi)[A']$ unsatisfiable.
- Clauses learned based on possible *non-QCDCL* assignments A'.
- Effects of QU-resolution in QCDCL.

Implementing Generalized Axioms in QCDCL

Dynamic Blocked Clause Elimination (QBCE): [LBB+15]

- Apply QBCE incrementally in QBCP by watched data structures.
- Empty formula: cube learning by generalized axiom.

Example ([LBB+15])

$\exists z,z' \forall u \exists y.$
$(u \vee \bar{y}) \wedge (\bar{u} \vee y) \wedge (z \vee u \vee \bar{y}) \wedge (z' \vee \bar{u} \vee y) \wedge (\bar{z} \vee \bar{u} \vee \bar{y}) \wedge (\bar{z}' \vee u \vee y)$

- Initially $A = \emptyset$ and no clause blocked in $\psi[A] = \psi$.
- For $A = \{\bar{z}, \bar{z}'\}$ all clauses blocked in $\psi[A] = \forall u \exists y.(u \vee \bar{y}) \wedge (\bar{u} \vee y)$.
- Derive $C = (\bar{z} \wedge \bar{z}')$ by generalized cube axiom and immediately $\emptyset$.
- Exponential cube proofs with traditional axiom:
  $\Phi(n) = \exists z_1,z_1' \forall u_1 \exists y_1, \ldots, \exists z_n,z_n' \forall u_n \exists y_n. \bigwedge_{i=1}^{n} \left[\mathcal{C}_0(i) \wedge \mathcal{C}_1(i) \wedge \mathcal{C}_2(i)\right]$,
  $\mathcal{C}_0(i) = (u_i \vee \bar{y}_i) \wedge (\bar{u}_i \vee y_i)$,
  $\mathcal{C}_1(i) = (z_i \vee u_i \vee \bar{y}_i) \wedge (z_i' \vee \bar{u}_i \vee y_i)$,
  $\mathcal{C}_2(i) = (\bar{z}_i \vee \bar{u}_i \vee \bar{y}_i) \wedge (\bar{z}_i' \vee u_i \vee y_i)$.

Experiments

Variants of DepQBF:

- DQ: only dynamic QBCE.
- DQ-T: + trivial truth.
- DQ-A: + abs. clause axiom.
- DQ-B: + Bloqqer.
- DQ-BAT: all listed above.

Solver	$\#T$	$\#U$	$\#S$	*Time*
DQ-BAT	466	236	230	553K
DQ-AT	461	234	227	555K
DQ-A	459	237	222	561K
DQ-B	449	222	227	563K
DQ-T	441	220	221	571K
DQ	441	224	217	575K
QELL-nc	434	302	132	563K
RAReQS	414	272	142	611K
CAQE	370	192	178	708K
GhostQ	347	166	181	752K
QESTO	331	188	143	767K

- QBF Gallery 2014 application benchmark set (735 formulas).
- Total solved ($\#T$), solved unsatisfiable ($\#U$), and satisfiable ($\#S$).
- No preprocessing by Bloqqer.

Experiments

Variants of DepQBF:

- DQ: only dynamic QBCE.
- DQ-T: + trivial truth.
- DQ-A: + abs. clause axiom.
- DQ-B: + Bloqqer.
- DQ-BAT: all listed above.

Solver	$\#T$	$\#U$	$\#S$	*Time*
QELL-nc	483	306	177	480K
DQ-AT	483	260	223	509K
DQ-A	481	262	219	528K
DQ-BAT	480	257	223	516K
RAReQS	471	272	199	509K
CAQE	465	248	217	534K
DQ-T	464	243	221	526K
DQ	456	242	214	542K
DQ-B	450	245	205	550K
QESTO	401	212	189	662K
GhostQ	306	148	158	823K

- QBF Gallery 2014 application benchmark set (735 formulas).
- Total solved ($\#T$), solved unsatisfiable ($\#U$), and satisfiable ($\#S$).
- Restricted preprocessing by Bloqqer (only QBCE and $\forall$ expansion).

Experiments

Variants of DepQBF:

- DQ: only dynamic QBCE.
- DQ-T: + trivial truth.
- DQ-A: + abs. clause axiom.
- DQ-B: + Bloqqer.
- DQ-BAT: all listed above.

Solver	$\#T$	$\#U$	$\#S$	*Time*
RAReQS	547	314	233	379K
QELL-nc	501	301	200	445K
QESTO	463	248	215	558K
DQ-AT	434	209	225	579K
DQ-BAT	432	209	223	585K
DQ-T	426	200	226	586K
DQ-A	418	207	211	623K
DQ-B	409	201	208	622K
DQ	407	200	207	623K
CAQE	401	193	208	640K
GhostQ	350	176	174	739K

- QBF Gallery 2014 application benchmark set (735 formulas).
- Total solved ($\#T$), solved unsatisfiable ($\#U$), and satisfiable ($\#S$).
- Full preprocessing by Bloqqer.

Experiments

Solver rankings: no (n), restricted (r), full preprocessing (f)			
Solver	*n*	*r*	*f*
CAQE	9	6	10
DQ	6	8	9
DQ-A	3	3	7
DQ-AT	2	2	4
DQ-B	4	9	8
DQ-BAT	1	4	5
DQ-T	5	7	6
GhostQ	10	11	11
QELL-nc	7	1	2
QESTO	11	10	3
RAReQS	8	5	1

- Three different winning solvers/approaches.
- Preprocessing may be harmful to the performance of certain solvers.

Conclusion and Outlook

Generalized Axioms in QRES:

- Derive clauses (cubes) other than input clauses (CNF models).
- Interface to combining QRES with orthogonal QBF proof systems.
- In QCDCL: incomplete QBF satisfiability check of $\psi[A]$.
- Applicable to any variant of QRES (long-distance, QU-, . . .).
- Proof search more complex due to additional proof rules (CR_n class).

Proof Generation:

- A clause (cube) C obtained by generalized axioms has a proof P (perhaps) in a proof system other than $QRES$.
- P is part of the final proof P' produced by QRES e.g. in QCDCL.
- Checking P' requires to check subproofs P in different proof systems.

References I

U. Bubeck and H. Kleine Büning.
Bounded Universal Expansion for Preprocessing QBF.
In J. Marques-Silva and K. A. Sakallah, editors, *SAT*, volume 4501 of *LNCS*, pages 244–257. Springer, 2007.

Olaf Beyersdorff, Leroy Chew, and Mikolás Janota.
Proof Complexity of Resolution-based QBF Calculi.
In *STACS*, volume 30 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 76–89. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015.

A. Biere.
Resolve and Expand.
In H. H. Hoos and D. G. Mitchell, editors, *SAT (Selected Papers)*, volume 3542 of *LNCS*, pages 59–70. Springer, 2004.

References II

V. Balabanov and J. R. Jiang.
Unified QBF certification and its applications.
Formal Methods in System Design, 41(1):45–65, 2012.

Valeriy Balabanov, Magdalena Widl, and Jie-Hong R. Jiang.
QBF Resolution Systems and Their Proof Complexities.
In *SAT*, volume 8561 of *LNCS*, pages 154–169. Springer, 2014.

M. Cadoli, A. Giovanardi, and M. Schaerf.
An Algorithm to Evaluate Quantified Boolean Formulae.
In *AAAI/IAAI*, pages 262–267, 1998.

E. Giunchiglia, M. Narizzano, and A. Tacchella.
Clause/Term Resolution and Learning in the Evaluation of Quantified Boolean Formulas.
J. Artif. Intell. Res. (JAIR), 26:371–416, 2006.

References III

Mikolás Janota.
On Q-Resolution and CDCL QBF Solving.
In *SAT*, volume 9710 of *LNCS*, pages 402–418. Springer, 2016.

Mikolás Janota and Joao Marques-Silva.
Expansion-based QBF solving versus Q-resolution.
Theor. Comput. Sci., 577:25–42, 2015.

H. Kleine Büning, M. Karpinski, and A. Flögel.
Resolution for Quantified Boolean Formulas.
Inf. Comput., 117(1):12–18, 1995.

Florian Lonsing, Fahiem Bacchus, Armin Biere, Uwe Egly, and Martina Seidl.
Enhancing Search-Based QBF Solving by Dynamic Blocked Clause Elimination.
In *LPAR*, volume 9450 of *LNCS*, pages 418–433. Springer, 2015.

References IV

Florian Lonsing, Uwe Egly, and Martina Seidl.
Q-Resolution with Generalized Axioms.
CoRR, abs/1604.05994, 2016.
Preprint of SAT 2016 proceedings version (to appear in LNCS, Springer) with appendix.

R. Letz.
Lemma and Model Caching in Decision Procedures for Quantified Boolean Formulas.
In U. Egly and C. G. Fermüller, editors, *TABLEAUX*, volume 2381 of *LNCS*, pages 160–175. Springer, 2002.

Florian Lonsing, Martina Seidl, and Allen Van Gelder.
The QBF Gallery: Behind the scenes.
Artif. Intell., 237:92–114, 2016.

References V

Anavai Ramesh, George Becker, and Neil V. Murray.
CNF and DNF Considered Harmful for Computing Prime Implicants/Implicates.
JAIR, 18(3):337–356, 1997.

Horst Samulowitz and Fahiem Bacchus.
Binary Clause Reasoning in QBF.
In *SAT*, volume 4121 of *LNCS*, pages 353–367. Springer, 2006.

Allen Van Gelder.
Contributions to the Theory of Practical Quantified Boolean Formula Solving.
In Michela Milano, editor, *CP*, volume 7514 of *Lecture Notes in Computer Science*, pages 647–663. Springer, 2012.

References VI

L. Zhang and S. Malik.
Conflict Driven Learning in a Quantified Boolean Satisfiability Solver.
In L. T. Pileggi and A. Kuehlmann, editors, *ICCAD*, pages 442–449. ACM, 2002.

L. Zhang and S. Malik.
Towards a Symmetric Treatment of Satisfaction and Conflicts in Quantified Boolean Formula Evaluation.
In P. Van Hentenryck, editor, *CP*, volume 2470 of *LNCS*, pages 200–215. Springer, 2002.