Non-CNF QBF Solving with QCIR

Charles Jordan
Graduate School of Information Science and Technology
Hokkaido University

Will Klieber
Software Engineering Institute
Carnegie Mellon University

Martina Seidl
Institute for Formal Models and Verification
Johannes Kepler University Linz

Abstract

While it is empirically confirmed folklore that conjunctive normal form (CNF) is not the ideal input format for QBF solvers, most tool developers and therefore also the users focus on formulas in this restricted structure. One important factor for establishing non-CNF solving is the input format. To overcome drawbacks of available formats, the QCIR format has recently been presented. The QCIR format is a circuit-based input format for quantified Boolean formulas which supports structure sharing. In contrast to previous formats, the representation is very compact, yet still easy to parse and to read for the human user.

In this paper, we analyze the QCIR format in detail and provide tools and benchmarks which, we hope, will make its usage attractive and motivate tool developers to support this format as well as users to formulate their encodings in this format.

Introduction

SAT solvers have made tremendous advances in recent years, and are now widely used in applications as general-purpose NP solvers (Biere et al. 2009). However, there are many applications where PSpace-complete problems must be solved and (assuming PSpace ̸= NP) these problems cannot be represented as compact SAT encodings. Analogous to SAT solvers and NP, QBF solvers can serve as general-purpose PSpace solvers.

Quantified Boolean formulas (QBF) extend propositional formulas by allowing explicit quantification (∃, ∀) over the propositional variables (Kleine Büning and Bubeck 2009). The problem of determining whether a particular QBF holds is complete for the complexity class PSpace, making them a promising host language for encoding and solving many important problems from verification and artificial intelligence (see Benedetti and Mangassarian 2008) for a survey). Recently, there has been significant progress in QBF in developing fast, practical QBF solvers (see for example, the recent report on the QBF Gallery (Lonsing, Seidl, and Van Gelder 2015)), but QBF solvers have not reached the same level of adoption as SAT solvers so far.

QBF tools have inherited the tradition of usually requiring formulas to be in conjunctive normal form (CNF) from SAT solvers. A propositional formula is in CNF if it is a conjunction of clauses. A clause is a disjunction of literals and a literal is a variable or a negated variable. Additionally, QBFs have a quantifier prefix which fixes the quantifier type of the variables occurring in the CNF. This formula structure is called prenex conjunctive normal form (PCNF). Any formula of arbitrary structure can be efficiently encoded in PCNF by introducing auxiliary variables—called Tseitin variables—which avoid an exponential blowup (Tseitin 1983).

However, this tradition of using normal forms limits the information available to the QBF solvers which might negatively impact the solving process. In contrast to SAT, where satisfiability checking problems have to be solved, a QBF solver has to solve validity checking problems (depending on the variable quantification) as well which is biased by restrictive structure of the CNF.

Therefore, the QCIR format (QBF Gallery 2014) was developed during the last QBF Gallery events. However, tools and benchmarks are not yet widely available—leading to the cycle that tools and applications do not support QCIR because it is not yet in common use. In this paper we present application benchmarks and synthetic benchmarks in QCIR, as well as tools that utilize QCIR. We hope that this serves to establish QCIR as the standard format for non-CNF QBF.

This paper is structured as follows. First, we introduce the QCIR format in detail, compare it to older formats, and give some motivation for why it is important to have a non-CNF format for QBF. Next we present a set of benchmarks stemming from reduction finding tasks. Then we introduce a fuzzer for the QCIR format which randomly generates QCIR formulas. In the context of CNF solving, such formulas are successfully used in the solver development process, and this practice be easily lifted to the non-CNF case. We consider some first experiments with our newly generated benchmarks before concluding with an outlook.

The QCIR Format

Currently, the standard input format for QBF is QDIMACS1, which has been used since the very earliest QBF

1http://www.qbflib.org/qdimacs.html

Copyright © 2015, Association for the Advancement of Artificial Intelligence (www.aaai.org). All rights reserved.
Table 1: Comparison of QBF input formats

To overcome the drawbacks of the available formats, the QCIR (Quantified CIRcuit) format was introduced as a joint community activity in the context of the QBF Gallery 2013. It was then refined and proposed as input format for the structural track of the QBF Gallery 2014, but unfortunately this track was canceled as not enough participating solvers were submitted to organize an interesting competition.

The format supports different variants of QBFs. Basically, gates are defined which are then used in the definitions of other gates. Various kinds of gates like and, or, ite, and xor gates are supported. Furthermore, there are special quantifier gates which allows to position quantifiers at any position in the formula. The definition of the gates also enables structure sharing, because a label of a gate may occur in arbitrarily many other definitions of gates. The detailed grammar of QCIR formulas is shown in Figure 1. The first line of a QCIR file is the format identifier (“#QCIR-14”), and any other line that starts with “#” is a comment.

As non-CNF formulas in prenex format suffice for many applications, the grammar in Figure 1 includes a convenient syntax (qblock-prefix) for specifying a quantifier prefix without the explicit introduction of quantifier gates. Figure 2 shows the general form of a formula in prenex form. An example of a prenex formula is shown in Figure 3.

The QCIR format requires that gate variables be defined before they are used in the definition of another gate. E.g., if the gate definitions include “g1 = and(v1, v2)” and

<table>
<thead>
<tr>
<th>property</th>
<th>QDIMACS</th>
<th>boole</th>
<th>qpro</th>
<th>QCIR</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix operators</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>non-CNF</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>non-NNF</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>non-PNF</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>structure sharing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>xor</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ite</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>resource alloc.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>textual var. names</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

\[
\text{qcir-file ::= format-id qblock-prefix output-stmt (gate-stmt nl)}^* \\
\text{format-id ::= #QCIR-14 nl} \\
\text{qblock-prefix ::= (free (var-list) nl)? qblock-quant*} \\
\text{qblock-quant ::= quant (var-list) nl} \\
\text{var-list ::= (var,)* var} \\
\text{lit-list ::= (lit,)* lit | } \epsilon \\
\text{output-stmt ::= output (lit) nl} \\
\text{gate-stmt ::= var = and (lit-list) | var = or (lit-list) | var = xor (lit, lit) | var = ite (lit, lit, lit) | var = quant (var-list; lit) } \\
\text{quant ::= exists | forall} \\
\text{var ::= (A string of ASCII letters, digits, and underscores)} \\
\text{lit ::= var | } \neg var \\
\text{nl ::= newline}
\]

Figure 1: Grammar of QCIR input format

\[
\text{forall(v1)} \\
\text{exists(v2, v3)} \\
\text{output(g3)} \\
\text{g1 = and(v1, v2)} \\
\text{g2 = and(-v1, -v2, v3)} \\
\text{g3 = or(g1, g2)}
\]

\[
\forall v_1. \exists v_2. \exists v_3. (v_1 \land v_2) \lor (\neg v_1 \land \neg v_2 \land v_3) \\
g_1 \quad g_2 \quad g_3
\]

Figure 3: Example of QCIR formula in prenex form
variant of the CEGAR-based solver RAReQS⁵.

**Benefit of Non-CNF Representation**

CNF is the standard for SAT solvers, and it works rather well in that domain. However, for QBF solvers, converting from a circuit representation to CNF can harm the performance of QBF solvers. The reason for this is that the Tseitin transformation for converting to CNF introduces only existentially quantified variables (not universally quantified variables) for the gates of the circuit. These existential Tseitin variables are effective in efficiently pruning the search space when searching for a satisfying assignment, but they provide less help when searching for a falsifying assignment. In other words, the Tseitin transformation makes it difficult for a solver to discover when no falsifying assignments exist. A SAT solver is untroubled by this, because it never cares whether any falsifying assignments exist. As an example of how CNF is harmful in QBF, consider the prenex formula

\[
\forall x, \exists y. \psi(x, y)
\]

This formula is trivially true. Assigning \( y \) to be true immediately makes the matrix of the formula true, regardless of \( \psi \). Under the Tseitin transformation, Equation 1 becomes:

\[
\forall X. \exists y. \bigvee_{g1 \in \{g1, \ldots, g_n\}} \bigwedge_{\text{clauses defining gate vars}}\bigwedge_{g1}(\exists x. x \oplus g1)
\]

Setting \( y \) to be true no longer immediately makes the matrix true. Instead, an assignment needs to include the gate variables and the universal variables \( X \) in order to satisfy the matrix. Experimental results (Ansótegui, Gomes, and Selman 2005; Zhang 2006) indicate that purely CNF-based QDPLL QBF solvers would, in the worst case, require time exponential in the number of variables in \( X \) to solve the CNF formula, even though the original problem (before translation to CNF) is trivial.

With a circuit representation, QBF solvers can introduce two variables for each gate, one existential and one universal. The existential variables are used in the normal Tseitin transformation to CNF, whereas the universal variables are used in the dual transformation to disjunctive normal form (DNF). This dual representation enables the solver to immediately detect that no falsifying assignments exist for the above formula. Experimental results indicate that this dual representation can greatly improve a QBF solver’s performance on real-world problems (Zhang 2006; Gouliaeva and Bacchus 2010; Klieber et al. 2010).

**Application: Reduction-Finding**

Recent QBF Gallery events included a class of application benchmark formulas that encode the problem of searching for certain complexity-theoretic reductions. These benchmark formulas are now available in QCIR format, and can be produced using the generator described in (Jordan and Kaiser 2013a) with the new option \(-qcir\) to produce QCIR formulas without CNF conversion.

⁵http://sat.inesc-id.pt/~mikolas/sw/rareqs-nn/
First we give a short introduction of the problem. See (Jordan and Kaiser 2013b) for details, definitions and comparisons of various approaches to this question.

Given decision problems $P$ and $Q$, a reduction from $P$ to $Q$ is a (relatively easy-to-compute) function $r$ satisfying

$$
\exists r \forall x : x \in P \iff r(x) \in Q.
$$

Of course, the general problem of determining whether a reduction exists between two problems is undecidable – as are most related questions. However, we can restrict attention to a limited (but sufficiently interesting) class of reductions and relax (2) to hold only for structures $x$ of size at most a given finite $n$. This results in a problem that is (in a sense) in $\Sigma^p_2$.

The formulas we use encode the problem of searching for simple quantifier-free reductions between the 2304 pairs of 48 different decision problems contained in NL. Some of the resulting problems are trivial and useful only for basic testing, but some seem quite hard – e.g., searching for simpler reductions for the Immerman-Szelepcsényi Theorem.

We provide three sets of problems:

- **red\_1133** 2304 formulas with very simple parameters ($k = 1, c = 1, n = 3$).
- **red\_1344** QCIR encodings of the benchmarks from the QBF Gallery ($k = 1, c = 3, n = 4$).
- **red\_hard** a small set of more challenging formulas.

The formulas are produced using (2). First, there are leading existential quantifiers corresponding to the possible contents of a parameterized reduction. Then, the universal variables correspond to the appropriate structure (e.g., graphs) on which the decision problem $P$ is defined. The leading existential variables occur only on the right-side of the iff – they are used only to determine whether $r(x) \in Q$. Depending on $P$, $Q$ and $n$, additional variables may be used to encode transitive closures. The structure of the inner formula depends on the formulas defining $P$ and $Q$.

As a concrete example, the QCIR formula `nreachq_reachqu_1133.qcir` corresponds to searching for an extremely simple reduction for the

![Figure 5: Semantics of QCIR format](image)

![Figure 6: Cactus plot for GhostQ on the red\_1133 family](image)

Immerman-Szelepcsényi Theorem but restricts attention to only graphs of size 3. In QCIR this has 75 quantified variables (including encoded transitive closures), while CNF conversion introduces additional variables – for a total of 1759 in the QDIMACS encoding of this problem.

We compared the new QCIR encoding of `red\_1133` to the existing QDIMACS encoding of these problems, running GhostQ on both encodings with a timeout of 10 seconds. As discussed in detail later in this paper, GhostQ has a preprocessor that attempts to reverse-engineer QDIMACS back into circuit form. However, this capability is limited, and it turned out to be largely ineffective for the QDIMACS version of the `red\_1133` benchmarks. On the QCIR encodings, GhostQ timed out on only 3 instances, whereas it timed out on 108 instances for the QDIMACS encodings. If the timeout is lowered to 1 second, GhostQ times out on 96 QCIR instances and 316 QDIMACS instances. Figure 6 show the relation between time limit and number of instances solved.

**Randomly Generated Benchmarks**

Randomly generated formulas play an important role in the development process of CNF-based SAT and QBF solvers (Brummayer, Lonsing, and Biere 2010). Such formulas are the basis for fuzz testing and model-based testing in order to automatically detect various kinds of defects in solvers. Especially corner cases which are easily overlooked...
Reverse Engineering CNF

At the present time, most of the benchmarks available for QBF are in the QDIMACS format. In order to make the QCIR format more attractive to solver developers, we have developed a reverse-engineering tool QCIR-CONV that takes a QDIMACS file and converts it to the QCIR format. For QDIMACS files that were converted to CNF from a circuit, this tool attempts to reconstruct the circuit. QCIR-CONV is based on the preprocessor originally developed as part of GhostQ. Recent related work for extracting structure from a CNF representation includes (Goultiaeva and Bacchus 2013). QCIR-CONV is available at:

http://www.cs.cmu.edu/%7ewkliieber/qcir-conv.py

Let us discuss how QCIR-CONV works. At a high level, QCIR-CONV looks for patterns in the QDIMACS file that reveal gate definitions. For example, the following clauses may correspond to the gate definition \( g = x_1 \lor \ldots \lor x_n \):\

\[
\begin{align*}
(-g \lor x_1 \lor \ldots \lor x_n) \\
(g \lor \neg x_1) \\
\vdots \\
(g \lor \neg x_n)
\end{align*}
\]

In order for this to be a valid gate definition, \( g \) must not be upstream (in the quantifier prefix) of any of the literals \( x_1, \ldots, x_n \). Additionally, if any of the literals \( x_1, \ldots, x_n \) (or their negations) had previously been committed as defining a gate, we must check that \( g \) does not appear in the sub-formula represented by such literals, to avoid constructing a circuit with a cycle. Furthermore, for a single literal \( g \), there might be multiple sets of clauses that could be used to define \( g \) as a gate. In this case, QCIR-CONV arbitrarily picks one of them (except that it gives lower priority to single-input gates, i.e., equivalences such as \( q \equiv x \)).

QCIR-CONV also looks for if-then-else gates. Consider a gate \( g = \text{ite}(s, x, y) \), where \( s \) is the ‘selector’ of the \text{ite} gate. Such a gate can be encoded in CNF as follows:

\[
\begin{align*}
\text{Implication} & \quad \text{Clause} \\
(s \land x) & \Rightarrow g \\
&s \land \neg x \lor \lor g \\
(s \land \neg x) & \Rightarrow \neg g \\
&s \lor \lor \lor \lor g \\
(-s \land y) & \Rightarrow \lor \lor \lor g \\
(-s \land \lor y) & \Rightarrow \lor \lor \lor \lor g
\end{align*}
\]

QCIR-CONV looks for four consecutive clauses of the above form to detect possible \text{ite} gates. (Within the group of four clauses, the clauses may appear in any order with respect to each other, and the literals in each clause may also appear in any order.) XOR gates are also found by the above process for finding \text{ITE} gates: \( \text{xor}(x, y) = \text{ite}(x, \neg y, y) \).

If the output of a gate occurs in only one polarity in the original formula (for example, if the gate doesn’t occur within the scope of a negation or similar gates such as XOR), then the Plaisted-Greenbaum transformation (Plaisted and Greenbaum 1986) can be used instead of the Tseitin transformation for converting a formula to CNF. QCIR-CONV currently does not attempt to reverse the Plaisted-Greenbaum transformation.

Outlook

We conclude this paper with two topics which are subject to ongoing research: (i) reverse engineering structure if only a CNF is given, and (ii) certification.

\footnote{available at http://fmv.jku.at/qcir}
Companions. Suppose that an existential variable $g$ is always 'accompanied' by a set of literals $C$ — i.e., every clause that contains the variable $g$ (in either its positive or negative form) also contains $C$. (This pattern was observed in several QBFLIB benchmarks.) For example, consider a formula $\Phi$ where $g$ occurs in exactly the following clauses: 
$$(\neg s \lor \neg g \lor a \lor b), (\neg s \lor g \lor \neg a), (\neg s \lor g \lor \neg b),$$
$$(\neg s \lor \neg g \lor z), (\neg s \lor g \lor \neg z)$$
In this example, $C = \{\neg s\}$. The first three clauses, if $\neg s$ is removed from them, conform to the pattern of a gate definition $g = a \lor b$. Further note that the truth value of $\Phi$ is unchanged if $\neg s$ is removed from these three clauses. It is conjectured that these superfluous literals were included in benchmarks because they helped early CNF QBF solvers to detect satisfying assignments. QCIR-Conv identifies whether a potential gate variable is always ‘accompanied’ by other literals, and if so, it accounts for them when trying to identify clauses that would constitute a gate definition.

Strategy Extraction
Some QBF solvers (e.g., (Balabanov and Jiang 2012; Goultiaeva, Gelder, and Bacchus 2011; Jussila et al. 2007; Niemetz et al. 2012)) are able to provide a strategy for the winning player, i.e., Skolem functions for the existential variables if the formula is true, or Herbrand functions for the universal variables if the formula is false. (Balabanov et al. 2015) developed such a strategy-extraction algorithm for a long-distance resolution QBF solver. The strategy maps each variable of the winning player to a formula in terms of the upstream variables of the opposing player. A slightly-modified version of the QCIR format is able to represent such strategies. In the QCIR grammar, for the definition of output-stmt, we replace output (lit) with output (varlist). All the variables belonging to the winning player would be listed in this output statement and defined by appropriate gate-stmts. Note that this allows subformulas to be defined once and shared over the strategies for multiple variables.

Acknowledgements
The authors would like to thank all the people who contributed to the specification of the QCIR format.

Martina Seidl was partially supported by the Austrian Science Fund (FWF) under grant S11408-N23. Will Klieber was partially supported by the Department of Defense under Contract FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, an FFRDC. Charles Jordan was partially supported by JSPS Kakenhi 15H00847, ‘Exploring the Limits of Computation (ELC)’.

References


Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense or other sponsors. This material has been approved for public release and unlimited distribution. DM-0003126.


Goultiaeva, A.; Gelder, A. V.; and Bacchus, F. 2011. A uniform approach for generating proofs and strategies for both true and false QBF formulas. In Proc. of the 22nd International Joint Conference on Artificial Intelligence (IJCAI 2011), 546–553. IJCAI/AAAI.


