A File Format for QBF Certificates

Daniel Kroening and Christoph M. Wintersteiger

Computer Systems Institute, ETH Zürich

1 The QB Certificate File Format

We propose a file format for certificates of QBF instances.

1.1 Preliminaries

Definitions A variable in any QBF problem is represented by its variable index; an integer in the range $[1, 2^{31}]$.

A *literal* is a variable in either negated or non-negated form. A literal is represented by an integer in the range $[-2^{31}, 2^{31}]\setminus\{0\}$, where negative numbers represent negated variables.

A *clause* is a disjunction of literals and is represented by a set of literals. No order of literals is assumed. Every clause implicitly has a clause index; all clauses of a QBF problem are numbered ascending in order of appearence in the according problem file. Clause indices are integers from the range $[1, 2^{32}]$.

The QBF problem is assumed to be given in a file that uses the QDIMACS format.

Basic Rules

Note: A NUMBER is always assumed to be an integer in the range $[1, 2^{32}]$, except for the VINDEX which refers to a variable index and thus is in the range $[1, 2^{31}]$.

1.2 Header

Every QB Certificate file is required to begin with an appropriate header line that contains the QBCertificate keyword.

I.e.,

```
\text{HEADER} \rightarrow \texttt{QBCertificate NL}.
```

1.3 Extensions

Based on the Extension Theorem in [1], we support extension rules. Instead of allowing the introduction of arbitray functions (which would be too hard to verify), we just allow two special types. An extension line has the format

```
EXTENSION \rightarrow ITE | AND.
```

where the first VINDEX defines a fresh variable that will be quantified existentially and in the scope of the innermost variable that appears in the extension.

If-Then-Else The If-Then-Else extension rule allows the introduction of a new variable that is defined to be the If-Then-Else of three existing variables. The If-Then-Else extension thus requires exactly three parameters:

ITE \rightarrow E VINDEX I LITERAL LITERAL LITERAL NL.

This rule will introduce four new clauses into the original formula; for w = ifx then a else b we introduce the clauses $(\neg w \lor \neg x \lor a), (\neg w \lor x \lor b), (w \lor \neg x \lor \neg a)$ and $(w \lor x \lor \neg b)$.

AND A new variable may be defined to be the logical AND of existing variables:

AND \rightarrow E VINDEX A { LITERAL } 0 NL.

The number of existing variables that are used in this definition is not limited, but the extension line must be terminated by a 0.

This rule will introduce n + 1 clauses into the original formula: $(\neg f \lor v_1)$ to $(\neg f \lor v_n)$ and $(f \lor \neg v_1 \lor \cdots \lor \neg v_n)$, where f is the new variable that depends on the existing variables v_i .

1.4 Resolution

Whenever a clause should be (q-)resolved against another, this must be listed in the certificate. The resolution line format is the same as used in traces for SAT–Solvers.

I.e.,

$RESOLUTION \rightarrow CINDEX$	
$(* ({ LITERAL } 0))$	
$\{ CINDEX \} 0 NL.$	

The first CINDEX in this rule defines the new clause index that the resolvent should be assigned. What follows is the resolvent (a sequence of LITERALS, terminated by a 0) and the antecedents that the desired resolvent can be calculated from (a sequence of CINDEXs, terminated by a 0). The actual order of the resolutions will be determined by the verifier via constraint propagation.

Note that a q-resolution step includes for all-reduction.

1.5 Conclusions

The last line in any QB Certificate is the conclusion line that states whether the original problem is to be proven valid or invalid. In case of an unsatisfiable problem the index of the clause which should be empty, must be given.

I.e.,

For valid instances, the model is to be supplied in the conclusion line. New variables have to be defined by extensions first. The conclusion line will then contain a set of equivalences e = n, where e is an original, existentially quantified variable and n is an extension variable. These equivalences are to be supplied as a set of VINDEX/LITERAL pairs in the conclusion line.

1.6 The QB Certificate

Having specified all the ingredients for a QB Certificate, we can now specify a complete QB Certificate as

{ RESOLUTION	$CERTIFICATE \rightarrow$	HEADER
		{ RESOLUTION
EXTENSION }		EXTENSION }
CONCLUSION.		CONCLUSION.

References

 Toni Jussila, Armin Biere, Carsten Sinz, Daniel Kroening, and Christoph M. Wintersteiger. A first step towards a unified proof checker for QBF. In *Proc. of SAT*. To Appear, 2007.