NAME

evaluator4 – on-the-fly model checking of MCL v4 formulas

SYNOPSIS

bcg_open [*bcg_opt*] *spec*[**.bcg**] [*cc_opt*] **evaluator4** [*evaluator_opt*] *prop*[**.mcl**]

or:

exp.open *spec*[**.exp**] [*cc_opt*] **evaluator4** [*evaluator_opt*] *prop*[**.mcl**]

or:

fsp.open [*fsp_opt*] *spec*[**.lts**] [*cc_opt*] **evaluator4** [*evaluator_opt*] *prop*[**.mcl**]

or:

lnt.open [*lnt_opt*] *spec*[**.lnt**] [*cc_opt*] **evaluator4** [*evaluator_opt*] *prop*[**.mcl**]

or:

lotos.open [*lotos_opt*] *spec*[**.lotos**] [*cc_opt*] **evaluator4** [*evaluator_opt*] *prop*[**.mcl**]

or:

seq.open *spec*[**.seq**] [*cc_opt*] **evaluator4** [*evaluator_opt*] *prop*[**.mcl**]

DESCRIPTION

evaluator4 takes two inputs:

- A Labelled Transition System, expressed either as a BCG graph *spec***.bcg,** a composition expression *spec***.exp,** an FSP program *spec***.lts,** an LNT program *spec***.lnt,** a LOTOS program *spec***.lotos,** or a sequence file *spec***.seq.**

- A temporal logic property, contained in the file *prop*[**.mcl**], expressed as a formula in the *MCL* version 4 language. See the **mcl**(LOCAL) manual page for a complete definition of the *MCL* version 4 language.

evaluator4 performs an on-the-fly verification of the temporal property on the given Labelled Transition System (LTS for short). The result of this verification (TRUE or FALSE) is displayed, possibly accompanied by a diagnostic (see OPTIONS below).

The verification method underlying **evaluator4** is based upon a translation of the model checking problem into the resolution of a Parameterized Boolean Equation System (PBES) [Mat98a], which is carried out by combining two simultaneous on-the-fly activities:

- Instantiation of the PBES to yield a plain Boolean Equation System (BES), using the approach proposed in [Mat98b].

- Resolution of the resulting BES, using the algorithms provided by the **caesar_solve_1**(LOCAL) library of OPEN/CAESAR (see the corresponding manual page and the article [Mat06] for details).

OPTIONS

The options *bcg_opt*, if any, are passed to **bcg_lib**(LOCAL).

The options *exp_opt*, if any, are passed to **exp.open**(LOCAL).

The options *fsp_opt*, if any, are passed to **fsp.open**(LOCAL).

The options *lnt_opt*, if any, are passed to **lnt.open**(LOCAL).

The options *lotos_opt*, if any, are passed to **caesar**(LOCAL) and to **caesar.adt**(LOCAL).

The options *seq_opt*, if any, are passed to **seq.open**(LOCAL).

The options *cc_opt*, if any, are passed to the C compiler.

The following options *evaluator_opt* are currently available:

-bes [*file*[**.bes**[*.ext*]]]
Print in *file*[**.bes**] or, if the file name argument is missing, in file **evaluator.bes**, a textual description of the BES corresponding to the evaluation of the formula on the LTS. If present, the extension *.ext* must correspond to a known file compression format (e.g., *.Z*, *.gz*, *.bz2*, etc.). In this case, the file containing the BES is compressed according to the corresponding format. The list of currently supported extensions and compression formats is given by the **$CADP/src/com/cadp_zip** shell-script. This option does not influence the evaluation of the formula. Not a default option.

−block Assume that the property is specified as a system of modal equations in a file *file*[**.blk**] that must be given as argument to **evaluator4** instead of *prop*[**.mcl**]. This option is mainly intended for debugging purposes. The format of the input file is undocumented and subject to future changes. Not a default option.

−acyclic
Evaluate the formula on the LTS using an algorithm optimized for acyclic graphs. If option **-dfs** is present (which is the case by default), the tool checks during verification whether the LTS contains cycles; if this is the case, an error message is displayed and the execution is aborted. If option **-bfs** is present, the tool may not always detect the presence of cycles in the LTS, and hence it may enter an infinite loop; in this case, it is the user's responsibility to ensure that the LTS is acyclic. If the formula is unguarded (see Section REMARKS of the **mcl**(LOCAL) manual page), which may yield a BES with cyclic dependencies between variables even if the LTS is acyclic, an error message is displayed and the execution is aborted. Not a default option.

−bfs Evaluate the formula on the LTS using a breadth-first search algorithm. Compared to **-dfs**, this option is generally slower, but produces diagnostics of smaller depth. If option **-acyclic** is present, the breadth-first search algorithm is optimized for reducing memory consumption: in particular, if the LTS is a sequence and the formula is dataless, the memory used for verification is bounded by the size of the formula (number of operators) and independent of the length of the sequence (number of transitions). Not a default option.

−dfs Evaluate the formula on the LTS using a depth-first search algorithm. Compared to **-bfs**, this option produces diagnostics of greater depth, but is generally faster and consumes less memory for certain classes of formulas (such as those shown in EXAMPLES OF TEMPORAL PROPERTIES below). Default option.

-diag [*diag*[**.bcg**]]
Generate a diagnostic in BCG format (see the **bcg**(LOCAL) manual page for details) explaining the truth value of the formula. The diagnostic is generated in the file *diag*[**.bcg**] or, if the file name

argument is missing, in the file **evaluator.bcg**. The BCG files containing diagnostics can be visualized using the **bcg_draw**(LOCAL) and **bcg_edit**(LOCAL) tools of CADP (see the respective manual pages for details). Diagnostics are (usually small) portions of the LTS on which the formula yields the same result as when it is evaluated on the whole LTS. If the diagnostic is a sequence of LTS transitions, it will also be displayed using the SEQ format (see the **seq**(LOCAL) manual page for the definition of this format). Not a default option.

−depend

Display the list of library files included (directly or transitively) in the file *prop*[**.mcl**] and stop. This list may be incomplete if the *MCL* formula is syntactically incorrect. If present, this option has precedence over all the other options. Not a default option.

−expand

Expand the macro definitions and the source files included as libraries in the file *prop*[**.mcl**], producing as output a file *prop***.xm**, and stop. This option is useful for debugging purposes. Not a default option.

−hide [−total | −partial | −gate] *hiding_filename*

Use the hiding rules defined in *hiding_filename* to hide (on-the-fly) the labels of *spec*. See the **caesar_hide_1**(LOCAL) manual page for a detailed description of the appropriate format for *hiding_filename*.

The **-total**, **-partial**, and **-gate** options specify the "total matching", "partial matching", and "gate matching" semantics, respectively. See the **caesar_hide_1**(LOCAL) manual page for more details about these semantics. Option **-total** is the default.

−rename [−total|−single|−multiple|−gate] *renaming_filename*

Use the renaming rules defined in *renaming_filename* to rename (on-the-fly) the labels of *spec*. See the **caesar_rename_1**(LOCAL) manual page for a detailed description of the appropriate format for *renaming_filename*.

The **-total**, **-single**, **-multiple**, and **-gate** options specify the "total matching", "single partial matching", "multiple partial matching", and "gate matching" semantics, respectively. See the **caesar_rename_1**(LOCAL) manual page for more details about these semantics. Option **-total** is the default.

As for the **bcg_labels**(LOCAL) tool, several hiding and/or renaming options can be present on the command line, in which case they are processed from left to right.

The hiding and renaming options are useful for converting the transition labels of *spec* on-the-fly in order to make them compatible with the LTS model on which *MCL* formulas are interpreted (see Section OVERVIEW OF THE MCL LANGUAGE of the **mcl**(LOCAL) manual page).

−labels Display a list of UNIX regular expressions (see the **regexp**(LOCAL) manual page for a detailed description of UNIX regular expressions), which over-approximate the set of visible LTS actions (transition labels) satisfying the action predicates occurring in the formula. In other words, if an action *a* satisfies some action predicate, then there exists a regular expression among those displayed by this option such that *a* matches it. Each regular expression is written on a separate line and is enclosed between double quotes, thus being compatible with the format of labels in hiding and renaming files (see the **caesar_hide_1**(LOCAL) or **caesar_rename_1**(LOCAL) manual pages for a description of these files).

The formula is not evaluated on *spec*. Not a default option.

−silent Execute silently. Opposite of **-verbose**. Default option.

-source *file*:*line*
Change the file name and line number displayed in error messages as if the formula was contained in file *file* starting at line *line* (instead of starting at line 1 in file *prop*[**.mcl**]). This option has effect only on the messages triggered by the errors occurring in the top-level file *prop*[**.mcl**]. The messages triggered by the errors occurring in the included libraries (if any) are left unchanged.

−stat Display statistical information about the resolution of the BES corresponding to the evaluation of the formula on the LTS. Not a default option.

−tauconfluence
Reduce the LTS on the fly modulo tau-confluence (a form of partial order reduction that preserves branching equivalence) while evaluating the formula. This option can be safely used only for verifying formulas adequate w.r.t. branching equivalence, i.e., whose evaluation yields the same result on all branching equivalent LTSs. For example, formulas belonging to the fragment ACTL-X (i.e., ACTL without the next time operators) are adequate w.r.t. branching equivalence [DV90]. In some cases, this option may improve speed and memory consumption significantly. Not a default option.

−verbose
Animate the user's screen, telling what is going on. Opposite of **-silent**. Default option is **-silent**.

−version
Display the current version number of the tool and stop. To be effective, this option should occur as the first argument in the *evaluator_opt* section of the command line. Subsequent options and/or arguments, if any, will be discarded. Not a default option.

−warning
Suppress all warning diagnostics, at the risk of leaving actual issues in the *MCL* formula undetected. Not a default option.

EXIT STATUS

Exit status is 0 if everything is alright, 1 otherwise.

DIAGNOSTICS

When the source file *prop*[**.mcl**] is erroneous, error messages are issued.

BIBLIOGRAPHY

[DV90] R. De Nicola and F. W. Vaandrager. "Action versus State based Logics for Transition Systems." Proceedings Ecole de Printemps on Semantics of Concurrency, LNCS v. 469, p. 407-419, 1990.

[Mat98a]
R. Mateescu. "Verification des proprietes temporelles des programmes paralleles." PhD Thesis, Institut National Polytechnique de Grenoble, April 1998. Available from http://cadp.inria.fr/publications/Mateescu-98-a.html

[Mat98b]
R. Mateescu. "Local Model-Checking of an Alternation-Free Value-Based Modal Mu-Calculus." Proceedings of the 2nd International Workshop on Verification, Model Checking and Abstract Interpretation VMCAI'98, 1998. Available from http://cadp.inria.fr/publications/Mateescu-98-b.html

[Mat06] R. Mateescu. "CAESAR_SOLVE: A Generic Library for On-the-Fly Resolution of Alternation-Free Boolean Equation Systems." Springer International Journal on Software Tools for Technology Transfer (STTT), v. 8, no. 1, p. 37-56, 2006. Full version available as INRIA Research Report RR-5948. Available from http://cadp.inria.fr/publications/Mateescu-06-a.html

AUTHORS

See the AUTHORS section of the **evaluator**(LOCAL) manual page.

OPERANDS

spec.**bcg**	BCG graph (input)
spec.**exp**	network of communicating LTSs (input)
spec.**lts**	FSP specification (input)
spec.**lnt**	LNT specification (input)
spec.**lotos**	LOTOS specification (input)
spec.**seq**	sequence file (input)
prop.**mcl**	regular mu-calculus formula (input)
diag.**bcg**	diagnostic in BCG format (output)
file.**bes**	BES in textual format (output)

FILES

$CADP/src/xtl/∗*.mcl*	predefined libraries (input)

SEE ALSO

bcg(LOCAL), **bcg_open**(LOCAL), **caesar.adt**(LOCAL), **caesar_graph**(LOCAL), **caesar_solve_1**(LOCAL), **caesar**(LOCAL), **evaluator**(LOCAL), **evaluator3**(LOCAL), **exhibitor**(LOCAL), **exp**(LOCAL), **exp.open**(LOCAL), **fsp.open**(LOCAL), **lnt.open**(LOCAL), **lotos**(LOCAL), **lotos.open**(LOCAL), **mcl**(LOCAL), **mcl3**(LOCAL), **mcl4**(LOCAL), **regexp**(LOCAL), **seq**(LOCAL), **seq.open**(LOCAL)

Additional information is available from the CADP Web page located at http://cadp.inria.fr

Directives for installation are given in files **$CADP/INSTALLATION_**∗.

Recent changes and improvements to this software are reported and commented in file **$CADP/HISTORY**.

BUGS

Please report bugs to Radu.Mateescu@inria.fr