COORDINATION 2024: Artefact submission for the paper #8

This document specifies the instructions for the AEC of COORDINATION 2024 for the evaluation of our artefact submission. We set a `Docker` container for `TRAC` in order to simplify the work of the AEC (the `README` file at https://github.com/loctet/TRAC contains the instructions for the manual installation procedure).

Table of content

1. Installation

Follow the instructions at https://docs.docker.com/ to install `Docker` on your system.

To install and run TRAC using `Docker`:

1. Pull the `Docker` image:

   ```
   docker pull loctet/trac_dafsms:v1
   ```

2. Run the container:

   ```
   docker run -it loctet/trac_dafsms:v1
   ```

   (you might need to run the above commands as `root`). The former command downloads the `Docker` image of `TRAC` while the latter starts a container with an interactive terminal.

---

2. Reproducibility

2.1 How Table 1 has been created

We now describe how the information in Table 1 of our COORDINATION has
been determined.
We recall that Table 1 reports how our framework captures the features of the smart contracts in the Azure repository described at the following links:

- Hello Blockchain
- Simple Marketplace
- Basic Provenance
- Digital Locker
- Refrigerated Transportation
- Asset Transfer
- Room Thermostat
- Defective Component Counter
- Frequent Flyer Rewards Calculator.

For each smart contract, the table below reports

- where the features are met in the `Solidity` implementation in the Azure repository
- the lines in the DAFSM model where the feature is captured (if at all)

Example (link to .sol)	Line in Code for the feature	How TRAC handle it
Simple Marketplace	BI : Lines 21 & 44	BI: Line 1, 2 & 6

Example (link to .sol)	Line in Code for the feature	How TRAC handle it
Hello Blockchain	BI: Lines 19 & 39	Bi: Line 1 & 3
Bazaar	ICI: BazaarItem (Line 78) ItemList(Line 40) BI : BazaarItem (Line 76) ItemList(Line 33)	
Ping Pong	BI : Line 16 & 67 ICI : Lines 18, 29, 41, 47, 77, 82 & 88	
Defective Component Counter	BI: Line 17 PP: Line 15	BI: Line 1 PP: Line 1
Frequent Flyer Rewards Calculator	BI : Line 20 PP : Line 18	BI: Line 1 PP: Line 1
Room Thermostat	PP : Line 16	PP: Line 1
Asset Transfer	BI : Line 18, PP: Line 49 RR : Lines 97 & 171	BI: Lines 1& 3 PP: Lines 2& 7 RR:
Basic Provenance	BI: Line 19 PP: Line 17, 26 RR : Line 38, 51	BI: Line 1 PP: Line 1, 2, 3 RR:
Refrigerated Transportation	BI: Line 32 PP: Line 28, 89 RR : Line 118, 143 MRP : Lines 33, 34, 119 & 142	BI: Line 1 PP: Line 1, 5 & 9 RR: MRP:
Digital Locker	BI : Line 21 PP: Lines 19, 68 RR : Lines 102,126, 127, 139 & 149 MRP : Lines 76, 91	BI: Line 1 PP: Line 1 RR: MRP:

2.2. How to check the well-formedness of the Azure benchmarks

The DAFSM models for each smart contract but for `Bazaar` and `Ping Pong` of the Azure repository can be found in the directory `Examples/dafsms_txt/azure`.

To check a model with `TRAC`, navigate to the directory `src` and execute the `Main.py` as done with the `Docker` commands below on the `simple-marketplace` smart contract:

```
cd src
python3 Main.py --filetype txt "azure/simplemarket_place"
```

The latter command produces the following output

```
   --Parsing Txt to generate Json file

   Checking the well formness of the model----

   (!) Verdict: Well Formed
```

reporting that the DAFSMs for the `simplemarket_place` is well formed. For the other smart contracts it is enough to execute the python script on the corresponding DAFSM.

2.3. How to check the randomly generated models

The 135 randomly generated models used in last part of Section 4 of our paper are in `src/Examples/random_txt/tests_dafsm_1` splitted in subfolders each containing 5 DAFSMs and a `list_of_files_info.csv` file with metadata on the DAFSMs (we detail the metadata). Our performance analysis can be reproduced by executing the following commands in the `Docker`:

```
performancecd src
python3 Random_exec.py tests_dafsms_1 --number_runs_per_each 10 --number_test_per_cpu 5 --time_out 300000000000
```

Note that the results may vary due to different hardware/software configurations than those we used (cf. page 12 of the paper).
The latter command above specifies the target directory `tests_dafsms_1`, the number of repetitions for each experiment, the number of experiments analyzed by each cpu, and the time out in nanoseconds. While running the checks further `csv` files will be generated and finally merged into a single file called `src/Examples/random_txt/tests_dafsm_1/merged_list_of_files_info.csv`. Notice if the target directory in the command above is not changed, this `csv` file will be overwritten at each execution. The current content of the `csv` files when starting the `Docker` contains the values plotted in Figures 2 and 3 of our paper.

The plots can be obtained by executing

```
python3 ./plot_data.py examples_1 --file merged_list_of_files_info --field num_states,num_transitions,num_paths --pl_lines participants_time,non_determinism_time,a_consistency_time,z3_running_time --shape 2d --type_plot scatter
```

in the `Docker`; the plots are `png` images saved in the directory `Examples/random_txt/tests_dafsms_1`.

---

3. Usage

3.1. Format of DAFSMs

The DAFSMs model (Definition 1 of our paper) is renderer in `TRAC` with a DSL which represents a DAFSM as sequences of lines, each specifying a transition of the DAFSM. We explain the format of transitions through the Simple Market Place contract (→ following Example 1 of our paper), which in our DSL is

```
_ {True} o:O > starts(c,string _description, int _price) {description := _description & price := _price} {string description, int price, int offer} S0
S0 {_offer > 0} b:B > c.makeOffer(int _offer) {offer := _offer} S1
S1 {True} o > c.acceptOffer() {} S2+
S1 {True} o > c.rejectOffer() {} S01
S01 {_offer > 0} any b:B > c.makeOffer(int _offer) {offer := _offer} S1
S01 {_offer > 0} b:B > c.makeOffer(int _offer) {offer := _offer} S1
```

hereafter called `SMP`; the names of states in `SMP` differ from those in Example 1, but this is immaterial for the analysis.

In general a transition consists of

- a source and a target state; a trailing `+` denotes final states (like `S2+` above)
- a guard specified in the notation of `Z3`
- a qualified participant `p : P` corresponding to *ν* p : P in the paper, `any p : P`, or just `p`
- a call to an operation of the contract
- a list of `&`-separate assignments.

The first line of `SMP` is a special transition corresponding to the edge entering the initial state in Example 1 barred for

- the fact that the source state is `_` is used to identify the initial state
- the additional `_description` parameter, omitted in the paper for readability

The guard `True` in the transition is the *precondition* while the list of assignments `{description := _description & price := _price}` is followed by an explicit declaration of the contract variables to capture the assumption in the first item of Page 3 of the paper; the transition introduces a fresh participant `o` with role `O` which renders the object-oriented mechanism described just above Definition 1.

Conventionally, parameters start with `_` to distinguish them from contract variables.

3.2. Examples of non well-formed models

As seen in section, `SMP` is well-formed; we now apply `TRAC` to detect non well-formed models. The file `azure/simplemarket_place_edit_1` contains a modified DAFSM obtained by replacing the `acceptOffer` transition of `SMP` with

`S1 {True} x > c.acceptOffer() {} S2+`

Executing in the `Docker`

```
python3 Main.py --filetype txt "azure/simplemarket_place_edit_1"
```

produces

```
The Path : _-starts-S0>S0-makeOffer-S1 does not contain the participant x : []
Error from this stage:S1_acceptOffer()_S2
--For _acceptOffer_0:   Check result ::  False
--- Participants       : False

(!) Verdict: Not Well Formed
```

stating that participant `x` has not been introduced. In fact, the `CallerCheck` finds a path to `S1` where participant `x` is not introduced (first line of the output above) identified in the trasition from `S1` to `S2` with label `acceptOffer` (second line of the output). The last three lines of the output inform the user that well formedness does not hold for the use of a non introduced participant.

The file `azure/simplemarket_place_edit_2` modifies `SMP` by replacing the transitions `acceptOffer` and `rejectOffer` respectively with

`S1 {False} o > c.acceptOffer() {} S01` and `S1 {False} o > c.rejectOffer() {} S01`

Executing now the command below in the `Docker`

```
python3 Main.py --filetype txt "azure/simplemarket_place_edit_2"
```

produces

```
Error from this state:S01_makeOffer(int _offer)_S1
--For _makeOffer_0:   Check result ::  False
--- A-Consistency: False

    Simplify of the Not Formula:  Not(And(Not(_offer <= 0), offer == _offer))  ::  True

    (!) Verdict: Not Well Formed
```

which tells that consistency is violated by the transition

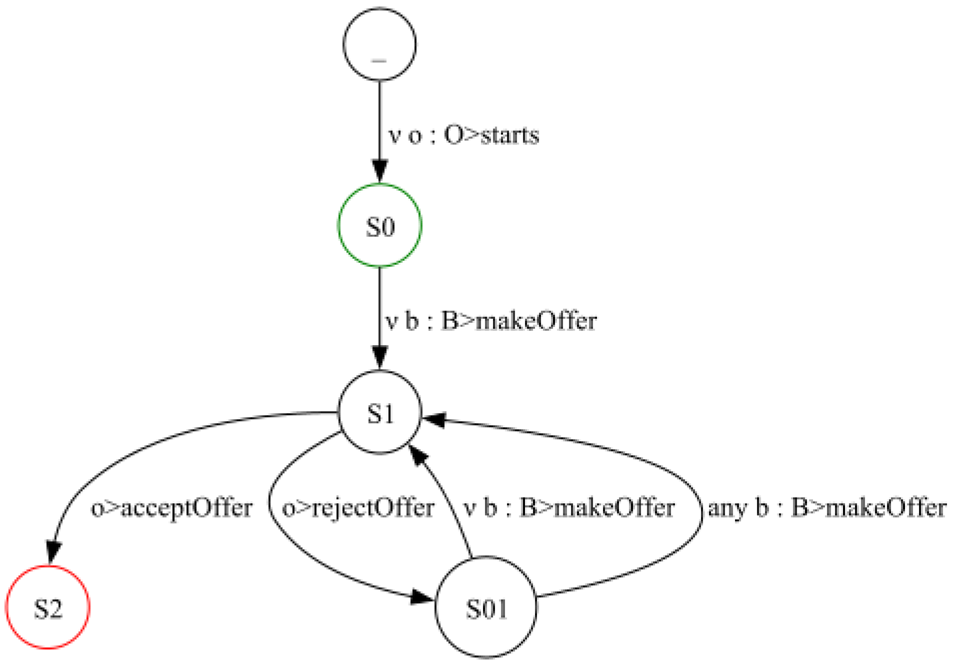
```
S0 {_offer > 0} b:B > c.makeOffer(int _offer) {offer := _offer} S1
```

The simplification operated by `Z3` on the formula in the last but one line of the output yields (the formula) `True`.

The `Main.py` script used above accepts the `check_type <chk>` optional parameters where `<chk>` can take two qualifiers; `check_type` defaults to `1` which checks well-formedness and can be set to `fsm` to generate a visual representation of a DAFSM as a `png` file. To access the file it is necessary to copy it from the `Docker` with the following command executed in a non-docker shell:

```
docker cp <container-ID>:<path-to-image> <destination-path-on-local-machine>
```

The image generated for `SMP` is below.



3.3. Commands for performance evaluation

To evaluate the performances of `TRAC`, we created a randomizer that contains a generator of random models in our DSL, a program that applies `TRAC` on the generated models, and a visualiser to plot data from `csv` files. In the following, we explain how to perform each step.

Generating random examples

The following command generates 100 random models and saves them in the directory `Examples/random_txt/your_sub_dir_name`:

```
python3 Generate_examples.py --directory your_sub_dir_name --num_tests 100
```

The generation process can be customised setting optional parameters of `Generate_examples.py`; if not specified, such parameters default to randomly generated values:

- `--num_tests` the number of tests to generate
- `--num_states` the number of states per test
- `--num_actions` the number of actions
- `--num_vars` the number of variables
- `--max_num_transitions` the maximum number of transitions
- `--max_branching_factor` the maximum branching factor
- `--num_participants` the number of participants
- `--incremental_gen` enables incremental generation with num_states ranging from 10 to num_tests with given steps
- `--merge_only_csv` merges results into a single CSV without generating new tests
- `--steps` the increment steps for generating tests
- `--num_example_for_each` the number of examples to generate for each configuration.

To generate the examples used in Section 4 of the paper, we ran the following command:

```
python3 Generate_examples.py --directory tests_dafsms_1 --steps 5 --num_example_for_each 5 --num_tests 30 --incremental_gen True
```

The above command creates 135 random examples in the directory `Examples/random_txt/tests_dafsms_1`, with a CSV containing metadata of each generated example. [The full description of the metadata list can be found here]

The check of the generated examples starts immediately after generation completion. This process allows the auto-generation and checking of DAFSMs examples, facilitating the evaluation of `TRAC`.

Running a set of examples

The following command configuration allows you to check a set of examples in a given sub-repository `<subdir>` in `Examples/random_txt`:

```
python3 Random_exec.py --directory <subdir> --number_test_per_cpu 5 --number_runs_per_each 10 --time_out 300000000000
```

The latter command takes all the examples metadata information in file `list_of_files_info.csv` in the `<subdir>`, allocates 5 examples to each CPU, and checks each example 10 times to have an average measured time, each CPU will output a CSV file `list_of_files_info_{id}.csv` at the end, and all generated csvs will be merged into `merged_list_of_files_info.csv` upon completion of all the examples.
The checking process can be customized setting some parameters of `Random_exec.py`. The full list of available parameters follows:

- `--merge_csv` only merges individual CSV results into `merged_list_of_files_info.csv`
- `--add_path` just count the number_path to each test in the `list_of_files_info.csv`
- `--number_test_per_cpu` determines how many tests are to run in parallel per CPU
- `--number_runs_per_each` specifies how many times to run each test
- `--time_out` sets a timeout limit for each test

The checking process splits tests for parallel execution, each thread output results into a CSV file and merges them upon completion. Results are stored in a subdirectory within `Examples/random_txt/<subdir>` to preserve data.

Plotting Results

To plot data using `Plot_data.py`, the following command can be customized with some given parameters below:

```
python3 Plot_data.py <directory> --shape <shape> --file <file_name> --fields <fields_to_plot> --pl_lines <lines_to_plot> --
type_plot <plot_type>
```

- `<directory>` the directory where the test data CSV is located, relative to `./Examples/random_txt/` where the `merged_list_of_files_info.csv` is
- `--shape` choose the plot shape: `2d`, `3d`, or `4d`
- `--file` specify the CSV file name without the extension, defaulting to `merged_list_of_files_info`
- `--fields` set the column(s) to plot against time, default is `num_states`
- `--pl_lines` define which time metric to plot against the fields, with defaults including participants' time, non-determinism time,and a-consistency-time
- `--type_plot` choose the type of 2D plot, with `line` (values `line`, `scatter`, `bar`)as the default
- `--scale` Y scale function, with default `log` (values `log`, `linear`).

To generate the plots of section 4 of the paper, we ran the following commands:

```
python3 Plot_data.py tests_dafsms_1 --file merged_list_of_files_info --field num_states,num_transitions,num_paths --pl_lines
participants_time,non_determinism_time,a_consistency_time,z3_running_time --shape 2d --type_plot scatter --scale linear

python3 Plot_data.py tests_dafsms_1 --file merged_list_of_files_info --field num_states,num_transitions,num_paths --pl_lines
participants_time,non_determinism_time,a_consistency_time,z3_running_time --shape 2d --type_plot scatter --scale log
```

This command allows different plotting configurations, adjusting for different dimensions and aspects of the data captured in the CSV file. All plots are saved in the directory `<directory>`.

3.4. Run your own examples

Now that the check of some examples is completed, you can design some DAFSMs and check if they are well-formed by giving the name of the file to the following command (`python3 Main.py --filetype txt "xxxxxxxxx"`)

/!\ All manually executed examples should be placed in the folder `Examples/dafsms_txt`. You can create sub-dirs, just be assured to run the above command with the exact name to the example `<subdir>/<example>`.

Some examples can be found in `Examples/other_tests` testing some scenarios which are not found in the Azure repository.

---

4. Documentation

The full documentation in HTML format can be downloaded [in from the git repository]

CSV Header Description

- `path` the path of the file
- `num_states` number of states in the FSM
- `num_actions` number of actions in the FSM
- `num_vars` number of variables in the FSM
- `max_branching_factor` maximum branching factor in the FSM
- `num_participants` number of participants in the FSM
- `num_transitions` number of transitions in the FSM
- `seed_num` seed number used for randomization
- `min_param_num` minimum number of parameters
- `average_param_num` average number of parameters
- `max_param_num` maximum number of parameters
- `min_bf_num` minimum number of branching factors
- `average_bf_num` average number of branching factors
- `max_bf_num` maximum number of branching factors
- `num_paths` number of paths in the FSM
- `verdict` verdict of the verification process
- `participants_time` time taken for checking participants
- `non_determinism_time` time taken for non-determinism check
- `a_consistency_time` time taken for action consistency check
- `f_building_time` time taken for formula building
- `building_time` time taken for building
- `z3_running_time` time taken for running Z3
- `total` total time taken for the process
- `is_time_out` indicates if there was a timeout during processing.

5. Tips

All commands provided, `Main.py`, `Generate_examples.py`, `Random_exec.py`, and `Plot_data.py`, come equipped with a `--help` option. Utilizing `--help` will display detailed usage instructions and available options for each command, aiding users in understanding and effectively utilizing the tool's features.

```
python3 Main.py --help
```