Optimizations and Correctness

Here we show what the differences of Rabinizer to [KE12] are and show the correctness.

1 Prototype of [KE12]

We first recall the construction of [KE12].

1.1 LTL Notation

We define a symbolic one-step unfolding $\mathfrak{U}$ of a formula inductively by the following rules.

$$\begin{aligned}
\mathfrak{U}(a) &= a \\
\mathfrak{U}(\neg a) &= \neg a \\
\mathfrak{U}(\varphi \wedge \psi) &= \mathfrak{U}(\varphi) \wedge \mathfrak{U}(\psi) \\
\mathfrak{U}(\varphi \vee \psi) &= \mathfrak{U}(\varphi) \vee \mathfrak{U}(\psi) \\
\mathfrak{U}(\mathbf{F}\varphi) &= \mathfrak{U}(\varphi) \vee \mathbf{XF}\varphi \\
\mathfrak{U}(\mathbf{G}\varphi) &= \mathfrak{U}(\varphi) \wedge \mathbf{XG}\varphi
\end{aligned}$$

In addition, $\mathbf{X}^{-1}(\psi)$ removes $\mathbf{X}$'s from ψ.

Let $\mathbb{F}$ and $\mathbb{G}$ denote the set of all subformulae of φ of the form $\mathbf{F}\psi$ and $\mathbf{G}\psi$, respectively. Further, all temporal subformulae are denoted by a shorthand $\mathbb{T} := \mathbb{F} \cup \mathbb{G}$. Finally, for a set of formulae Ψ, we denote $\mathbf{X}\Psi := \{\mathbf{X}\psi \mid \psi \in \Psi\}$.

1.2 Muller Automaton

We denote the *closure* of φ by $\mathbb{C}(\varphi) := Ap \cup \{\neg a \mid a \in Ap\} \cup \mathbf{X}\mathbb{T}$. Then $\mathfrak{U}(\varphi)$ is a positive Boolean combination over $\mathbb{C}(\varphi)$. By states(φ) we denote the set $2^{2^{\mathbb{C}(\varphi)}}$. Each element of states(φ) is a positive Boolean function over $\mathbb{C}(\varphi)$ and we often use a positive Boolean formula as its representative. For instance, the definition of $\mathfrak{U}$ is clearly independent of the choice of representative, hence we abuse the notation and apply $\mathfrak{U}$ to elements of states(φ).

Consider a formula χ as a Boolean function over elements of $\mathbb{C}(\varphi)$. For sets $T, F \subseteq \mathbb{C}(\varphi)$, let $\chi[T \mapsto \mathbf{tt}, F \mapsto \mathbf{ff}]$ denote the formula where $\mathbf{tt}$ is substituted for elements of T, and $\mathbf{ff}$ for F. As elements of $\mathbb{C}(\varphi)$ are considered to be atomic expressions here, the substitution is only done on the propositional level and does not go through the modality, e.g. $(a \vee \mathbf{XG}a)[a \to \mathbf{ff}] = \mathbf{ff} \vee \mathbf{XG}a$, which is equivalent to $\mathbf{XG}a$ in the propositional semantics.

Our state space has two components. Beside the logical component, we also keep track of one-step history of the word read. We usually use letters ψ, χ when speaking about the former component and α, β for the latter one.

Definition 1. *Given a formula φ, we define $\mathcal{A}(\varphi) = (Q, i, \delta)$ to be a deterministic finite automaton over $\Sigma = 2^{Ap}$ given by*

- *the set of states* $Q = \{i\} \cup \Big(\text{states}(\varphi) \times 2^{Ap}\Big)$
- *the initial state* i*;*
- *the transition function*

$$\delta = \{\big(i, \alpha, \langle \mathfrak{U}(\varphi), \alpha\rangle\big) \mid \alpha \in \Sigma\} \cup \{\big(\langle \psi, \alpha\rangle, \beta, \langle \text{succ}(\psi, \alpha), \beta\rangle\big) \mid \langle \psi, \alpha\rangle \in Q, \beta \in \Sigma\}$$

where $\text{succ}(\psi, \alpha) = \mathfrak{U}(\mathbf{X}^{-1}(\psi[\alpha \mapsto \mathbf{tt}, Ap \setminus \alpha \mapsto \mathbf{ff}])$.

1.3 Muller Acceptance Condition

For a formula χ and $\alpha \in \Sigma$ and $I \subseteq \mathbb{T}$, we put $I \models_\alpha \chi$ to denote that

$$\chi[\alpha \cup I \mapsto \mathbf{tt}, Ap \setminus \alpha \mapsto \mathbf{ff}]$$

is equivalent to $\mathbf{tt}$ in the propositional semantics. We use this notation to describe that we rely on a commitment to satisfy all formulae of I.

Definition 2 (Muller acceptance). *A set $M \subseteq Q$ is* Muller accepting for a set $I \subseteq \mathbb{T}$ *if the following is satisfied:*

1. *for each $(\chi, \alpha) \in M$, we have $\mathbf{X}I \models_\alpha \chi$,*
2. *for each $\mathbf{F}\psi \in I$ there is $(\chi, \alpha) \in M$ with $I \models_\alpha \psi$,*
3. *for each $\mathbf{G}\psi \in I$ and for each $(\chi, \alpha) \in M$ we have $I \models_\alpha \psi$.*

A set $F \subseteq Q$ is Muller accepting (for φ) *if it is Muller accepting for some $I \subseteq \mathbb{T}$.*

The first condition ensures that the commitment to formulae in I being ultimately satisfied infinitely often is enough to satisfy the requirements. The second one guarantees that each $\mathbf{F}$-formula is unfolded only finitely often and then satisfied, while the third one guarantees that $\mathbf{G}$-formulae indeed ultimately hold. Note that it may be impossible to see the satisfaction of a formula directly and one must rely on further promises, formulae of smaller size. In the end, promising the atomic proposition is not necessary and is proven directly from the second component of the state space.

1.4 Generalized Rabin Condition

A *generalized Rabin automaton* is a (deterministic) ω-automaton $\mathcal{A} = (Q, i, \delta)$ over some alphabet Σ, where Q is a set of states, i is the initial state, $\delta : Q \times \Sigma \to Q$ is a transition function, together with a *generalized Rabin condition* $\mathcal{GR} \in \mathcal{B}^+(2^Q \times 2^Q)$. A run ρ of $\mathcal{A}$ is accepting if $\text{Inf}(\rho) \models \mathcal{GR}$, which is defined inductively as follows:

$$\begin{aligned}
\text{Inf}(\rho) &\models \varphi \wedge \psi && \iff \text{Inf}(\rho) \models \varphi \text{ and } \text{Inf}(\rho) \models \psi \\
\text{Inf}(\rho) &\models \varphi \vee \psi && \iff \text{Inf}(\rho) \models \varphi \text{ or } \text{Inf}(\rho) \models \psi \\
\text{Inf}(\rho) &\models (F, I) && \iff F \cap \text{Inf}(\rho) = \emptyset \text{ and } I \cap \text{Inf}(\rho) \neq \emptyset
\end{aligned}$$

Definition 3 (Generalized Rabin Acceptance). *Let φ be a formula. The* generalized Rabin condition $\mathcal{GR}(\varphi)$ *is*

$$\bigvee_{I \subseteq \mathbb{T}} \left(\left(\{(\chi, \alpha) \mid I \not\models_\alpha \chi \wedge \bigwedge_{\mathbf{G}\psi \in I} \psi\}, Q \right) \wedge \bigwedge_{\mathbf{F}\omega \in I} \left(\emptyset, \{(\chi, \alpha) \mid I \models_\alpha \omega\} \right) \right)$$

2 Rabinizer

The most important optimizations are the following.

1. The evolution of the first component containing the formula to be satisfied has been altered. In the original approach, in order to obtain the acceptance condition easily, not all known information has been reflected immediately in the state space thus resulting in redundant "intermediate" states.
2. The generalized Rabin condition is now subject to several optimizations. Firstly, conjunctions of "compatible" Rabin pairs are merged into single pairs thus reducing the blowup from generalized Rabin to Rabin automaton. Secondly, some subformulae, such as outer **F** subformulae, are no more considered in the acceptance condition. For example, no infinite behaviour needs to be checked for $\mathbf{F}(a \wedge \mathbf{F}b)$.
3. The one-step history now does not contain full information about the letters, but only equivalence classes of letters. The quotienting is done in the coarsest way to still reflect the acceptance condition. A simple example is a formula $\varphi = \mathbf{GF}(a \vee b)$ where we only distinguish between reading any of $\{\{a\}, \{b\}, \{a, b\}\}$ and reading $\emptyset$.
4. The blow-up of the generalized Rabin automaton into a Rabin automaton has been improved. Namely, the copies of the original automaton are now quotiented one by one according to the criterion above, but only the conjuncts corresponding to a particular copy are taken into account. Thus we obtain smaller (and different) copies.
   Further, linking of the copies is now made more efficient. Namely, the final states in all but one copy have been removed completely.
5. No special state is dedicated to be initial without any other use. Although this results only in a decrease by one, it plays a role in tiny automata.

We now comment on these in more detail.

2.1 Optimization 1

The optimized transition function δ is given by

$$\langle \psi, \alpha \rangle \xrightarrow{\beta} \langle \mathbf{X}^{-1} \circ \mathfrak{U}(\psi)[\beta \mapsto \mathbf{tt}, Ap \setminus \beta \mapsto \mathbf{ff}], \beta \rangle$$

and the initial state is changed to $\langle \varphi, ? \rangle$.

Correctness For $M \subseteq Q$, denote M_{states} the projection on the first component and M_{Ap} on the second one. Further, for $\alpha \subseteq Ap$, we use a shorthand $\chi[\alpha] := \chi[\alpha \mapsto \mathbf{tt}, Ap \setminus \alpha \mapsto \mathbf{ff}]$. Using this notation, the acceptance condition can now be rewritten in a simpler way as follows.

A set $M \subseteq Q$ is *Muller accepting for a set* $I \subseteq \mathbb{T}$ if the following is satisfied:

1. for each $\chi \in M_{\text{states}}$, we have $I \models \chi$,
2. for each $\mathbf{F}\psi \in I$ there is $\alpha \in M_{Ap}$ with $I \models_\alpha \psi$,
3. for each $\mathbf{G}\psi \in I$ and for each $\alpha \in M_{Ap}$ we have $I \models_\alpha \psi$.

Optimization 1 only changes M_{states}. Every run $\rho_{\mathsf{old}}(w)$ of the old version

$$i \xrightarrow{\alpha_1} \langle \chi_1 := \mathfrak{U}(\varphi), \alpha_1 \rangle \xrightarrow{\alpha_2} \langle \chi_2 := \mathfrak{U}\mathbf{X}^{-1}(\chi_1[\alpha_1]), \alpha_2 \rangle \cdots \xrightarrow{\alpha_i} \langle \chi_i := \mathfrak{U}\mathbf{X}^{-1}(\chi_{i-1}[\alpha_{i-1}]), \alpha_i \rangle \cdots$$

can be mapped to a run $\rho'(w)$ of the optimized version

$$\langle \varphi, ? \rangle \xrightarrow{\alpha_1} \langle \chi'_1 := \mathbf{X}^{-1}(\mathfrak{U}(\varphi)[\alpha_1]), \alpha_1 \rangle \xrightarrow{\alpha_2} \langle \chi'_2 := \mathbf{X}^{-1}(\mathfrak{U}(\chi'_1)[\alpha_2]), \alpha_2 \rangle \cdots \xrightarrow{\alpha_i} \langle \chi'_i := \mathbf{X}^{-1}(\mathfrak{U}(\chi'_{i-1})[\alpha_i]), \alpha_i \rangle \cdots$$

By induction, $\chi'_i = \mathbf{X}^{-1}(\chi_i[\alpha_i])$, we have a bijection on the runs. The acceptance holds for the same M and I:

Condition 1.: $\mathbf{X}I \models_\alpha \chi$ iff $I \models \mathbf{X}^{-1}(\chi[\alpha])$ iff $I \models \chi'$.

Conditions 2. and 3. stay unaffected.

2.2 Optimization 2

All disjuncts in the generalized Rabin condition are of the form $(F, \bigwedge_{k \in K} I_k)$ that we call a *generalized pair*. Optimizations are performed in the following order.

1. Whenever there is a generalized pair $(F \cup \{x\}, \mathcal{I} \wedge (I \cup \{x\}))$ we replace it by $(F \cup \{x\}), \mathcal{I} \wedge I)$.
2. Whenever there is a generalized pair $(F, \mathcal{I} \wedge I \wedge J)$ with $I \subseteq J$ we replace it by $(F, \mathcal{I} \wedge I)$.
3. Whenever there is a generalized pair $(F, \emptyset)$ it is removed.
4. Whenever there is a generalized pair $(\bar{Q}, \mathcal{I})$ where $\bar{Q}$ is the reachable state space, it is removed.
5. Whenever there are generalized pairs $(F, \bigwedge_{k \in K} I_k)$ and $(F', \bigwedge_{k' \in K'} I'_{k'})$ such that $F \subseteq F'$ and for each $k' \in K'$ there is $k \in K$ with $I'_{k'} \subseteq I_k$, then the latter pair is removed.

Correctness

1. A run with infinitely many x's is always rejected by the pair.
2. When I occurs infinitely often so does J.
3. $\emptyset$ cannot be visited (infinitely often).
4. The whole state space cannot be avoided.
5. Whenever a run is accepted by the primed pair it is also accepted by the unprimed pair.

Optimization 2 - 2nd part

Let $\mathbb{F}'$ be the set of formulae $\psi \in \mathbb{F}$ that are not a subformula of any $\chi \in \mathbb{G}$. The set $\mathbb{T}$ in Definition 3 is replaced by $\mathbb{T} \setminus \mathbb{F}'$.

Correctness Let ρ be a run accepted by the original automaton and $\psi \in \mathbb{F}'$.

First case: only finitely many states in ρ contain an occurrence of ψ. Then ρ is accepted with a Muller accepting set for some $I \not\ni \psi$. Then the according pair appears in the optimized condition.

Second case: ψ appears in ρ infinitely often. Since there is no superformula $\chi \in \mathbb{G}$ that would generate it, either ψ or some superformula $\psi' \in \mathbb{F}$ has never been satisfied. In the former case, I cannot contain ψ as it is not satisfied infinitely often. In the latter case, $I \setminus \{\psi\}$ also guarantees acceptance as the run is accepting even when ψ' is replaced by $\mathbf{ff}$.

2.3 Optimization 3

For a (generalized) Rabin condition $\mathcal{R}$, let $\mathcal{S}(\mathfrak{R})$ denote the set of all sets in all (generalized) pairs.

Two valuations ν, ν' are equivalent w.r.t. a (generalized) Rabin condition $\mathfrak{R}$, written $\nu \sim_{\mathfrak{R}} \nu'$ if for all $S \in \mathcal{S}(\mathfrak{R})$ we have either $\nu \in S, \nu' \in S$ or $\nu \notin S, \nu' \notin S$.

The second component of each state is now an equivalence class of $\sim_{\mathfrak{R}}$.

Correctness Since only states with the same first component are merged, it follows that the behaviour of the automaton is correctly defined (transitions to successors of merged states are the same).

Further, obviously the acceptance condition cannot distinguish between two runs with the same $\sim_{\mathfrak{R}}$-projection.

2.4 Optimization 4

Whenever there is a generalized pair $(F, \bigwedge_{k \in K} I_k)$, we degeneralize it as follows. We change the state space into $Q \times K$. Intuitively, in the kth copy, we wait for visiting I_k. Whenever we are taking a transition to visit it, we move to the equivalent state of the next copy instead. The formal definition is straightforward. The pair is then replaced by $(F \times K, I_i)$ for an arbitrary fixed $i \in K$ (we set $i = 0$).

Firstly, we collapse the kth copy w.r.t. the condition where all I_ℓ's for $\ell \neq k$ are not taken into account.

Secondly, we do a transitive closure of the to-the-next-copy edges. More precisely, whenever an edge $(q, i) \to (r, i + 1)$ is produced and $r \in I_{i+1}$ then we prolong it to the equivalent state in the $(i + 2)$nd copy etc. Edges to the 0th copy do not get prolonged.

Correctness Firstly, visiting I_ℓ in the kth copy does not change the run. Secondly, the only accepting states are in the 0th copy and these are never skipped, as the edges to them never get prolonged.

2.5 Optimization 5

We start the construction with the initial state $(\varphi, ?)$ and when we find the first state of the form (φ, α) we set ? to α and reuse the initial state.

Correctness The only difference is that α is visited one more time, but this does not affect whether α is visited finitely or infinitely often.

References

[KE12] Jan Křetínský and Javier Esparza. Deterministic automata for the (F,G)-fragment of LTL. In *CAV*, 2012. To appear.