Counterexample-Guided Interval Weakening
Full Proofs and Pseudocode

Ben M. Andrew(✉), Marie Farrell, Louise A. Dennis, and Michael Fisher

Department of Computer Science, University of Manchester, UK
benjamin.andrew@manchester.ac.uk

Abstract. This is accompanying material to the paper *Counterexample-Guided Interval Weakening*, containing full proofs and pseudocode that could not fit into page limits.

1 Weakening Within Contexts

We briefly state the syntax and semantics of Metric Temporal Logic [2] (MTL). Let $\mathcal{P}$ be a set of propositional variables. Well-formed MTL formulae are formed according to the rule:

$$\phi := p \mid \top \mid \neg\phi \mid \phi \wedge \phi \mid \phi \,\mathcal{U}_I\, \phi \mid \phi \,\mathcal{R}_I\, \phi \tag{1}$$

where $p \in \mathcal{P}$ and I is an interval, $[a, b]$, for $a \in \mathbb{N}$ and $b \in \mathbb{N} \cup \{\infty\}$ and $a \leq b$. Other constructs can be defined as usual, e.g. $\Diamond_I \phi = \top \,\mathcal{U}_I\, \phi$. While the release operator $\mathcal{R}$ can be defined in terms of the until operator $\mathcal{U}$, this would leave a negation as the outermost operator, complicating our weakening algorithm. We consider MTL formulae with a pointwise semantics over the natural numbers [1], defined according to a trace π which is an infinite sequence of states in which atomic propositions can hold, and an index of the trace $t \in \mathbb{N}$. The set of atomic propositions that hold in the t-th state is denoted by $\pi(t)$. A trace π satisfies an MTL formula ϕ, denoted by $\pi \vDash \phi$, if and only if $\pi, 0 \vDash \phi$.

$$\begin{aligned}
&\pi, t \vDash p && \text{iff} \quad p \in \pi(t) \\
&\pi, t \vDash \neg\phi && \text{iff} \quad \pi, t \nvDash \phi \\
&\pi, t \vDash \phi_1 \wedge \phi_2 && \text{iff} \quad \pi, t \vDash \phi_1 \text{ and } \pi, t \vDash \phi_2 \\
&\pi, t \vDash \phi_1 \,\mathcal{U}_I\, \phi_2 && \text{iff} \quad \exists i \in I.\, ((\pi, t + i \vDash \phi_2) \wedge \forall j \in [0, i) \cap I.\, (\pi, t + j \vDash \phi_1)) \\
&\pi, t \vDash \phi_1 \,\mathcal{R}_I\, \phi_2 && \text{iff} \quad \forall i \in I.\, (\pi, t + i \vDash \phi_1) \\
& && \quad \vee \exists i \in I.\, (\pi, t + i \vDash \phi_2 \wedge \forall j \in [0, i] \cap I.\, (\pi, t + j \vDash \phi_1))
\end{aligned}$$

CEGIW weakens a constituent subformula of a larger formula. We show, using the notion of *contexts*, that a weakening of a subformula implies a weakening of the larger formula.

Definition 1 (Contexts). *MTL Contexts are like MTL formulae with a single hole* $[-]$*, and are formed according to the rule:*

$$C ::= [-] \mid C \wedge \phi \mid \phi \wedge C \mid C \vee \phi \mid \phi \vee C \mid C \,\mathcal{U}_I\, \phi \mid \phi \,\mathcal{U}_I\, C \mid C \,\mathcal{R}_I\, \phi \mid \phi \,\mathcal{R}_I\, C \tag{2}$$

where ϕ is an MTL formula and I is an interval. Our definition of contexts does not allow negations on the path to the hole $[-]$, similarly to the restriction imposed by negation normal form (NNF). However, adjacent MTL subformulae ϕ are not required to be in NNF and can contain negations.

We define the notion of *context substitution*, where an MTL formula ψ is substituted into the hole of a context C to produce an MTL formula $C[\psi]$.

$$\begin{aligned}
[-][\psi] &= \psi \\
(C \wedge \phi)[\psi] &= C[\psi] \wedge \phi & (C\, \mathcal{U}_I\, \phi)[\psi] &= C[\psi]\, \mathcal{U}_I\, \phi \\
(\phi \wedge C)[\psi] &= \phi \wedge C[\psi] & (\phi\, \mathcal{U}_I\, C)[\psi] &= \phi\, \mathcal{U}_I\, C[\psi] \\
(C \vee \phi)[\psi] &= C[\psi] \vee \phi & (C\, \mathcal{R}_I\, \phi)[\psi] &= C[\psi]\, \mathcal{R}_I\, \phi \\
(\phi \vee C)[\psi] &= \phi \vee C[\psi] & (\phi\, \mathcal{R}_I\, C)[\psi] &= \phi\, \mathcal{R}_I\, C[\psi]
\end{aligned} \tag{3}$$

By pushing negations inwards, an MTL formula ϕ can always be transformed into a context C and subformula ψ where ϕ is logically equivalent to $C[\psi]$.

Definition 2 (Weakening and strengthening of MTL formulae). *Let ϕ and ϕ' be MTL formulae. ϕ' is a weakening of ϕ, denoted*

$$\phi \sqsubseteq \phi' \tag{4}$$

if and only if, for all traces π and time-points t, if $\pi, t \vDash \phi$, then $\pi, t \vDash \phi'$. In this case, symmetrically, ϕ is a strengthening of ϕ'. Note that an MTL formula ϕ is always both a strengthening and a weakening of itself, i.e. $\phi \sqsubseteq \phi$.

Theorem 3 (Weakening of contexts). *Let C be a context and ψ and ψ' be MTL formulae. If $\psi \sqsubseteq \psi'$, then $C[\psi] \sqsubseteq C[\psi']$.*

Proof. We do an induction proof over the grammar of contexts using the induction hypothesis $P(C)$, that $C[\psi] \sqsubseteq C[\psi']$. The non-temporal inductive cases are omitted for brevity.

- Base case $[-]$: We assume that $\psi \sqsubseteq \psi'$, and by the definition of context substitution we have that $[-][\psi] \sqsubseteq [-][\psi']$ and thus $P([-])$.
- Inductive case $C\, \mathcal{U}_I\, \phi$: Assuming $P(C)$, we take an arbitrary trace π and time-point t, assume $\pi, t \vDash C[\psi]\, \mathcal{U}_I\, \phi$, and want to prove $\pi, t \vDash C[\psi']\, \mathcal{U}_I\, \phi$. We know that there exists an $i \in I$ such that $\pi, t + i \vDash \phi$, and that for all $j \in [0, i) \cap I$ we have $\pi, t + j \vDash C[\psi]$. Taking arbitrary i and j, by the induction hypothesis we have that $\pi, t + j \vDash C[\psi']$, and so by the semantics $\pi, t \vDash C[\psi']\, \mathcal{U}_I\, \phi$. Thus, we have $P(C\, \mathcal{U}_I\, \phi)$.
- Inductive case $\phi\, \mathcal{U}_I\, C$: Similar to the above case.
- Inductive case $C\, \mathcal{R}_I\, \phi$: Assuming $P(C)$, we take an arbitrary trace π and time-point t, assume $\pi, t \vDash C[\psi]\, \mathcal{R}_I\, \phi$, and want to prove $\pi, t \vDash C[\psi']\, \mathcal{R}_I\, \phi$. By the semantics of $\mathcal{R}$ there are two cases:
  1. For all $i \in I$ we have $\pi, t + i \vDash \phi$, thus we have $\pi, t + i \vDash C[\psi']$, and so we have $\pi, t \vDash C[\psi']\, \mathcal{R}_I\, \phi$.

2. There exists an $i \in I$ such that $\pi, t+i \vDash C[\psi]$, and that for all $j \in [0,i] \cap I$ we have $\pi, t+j \vDash \phi$. Taking arbitrary i and j, by the assumptions we have that $\pi, t+i \vDash C[\psi']$ and $\pi, t+j \vDash \phi$, and then by the semantics we have $\pi, t \vDash C[\psi'] \mathcal{R}_I \phi$.

Thus, in both cases we have $P(C \mathcal{R}_I \phi)$.

INDUCTIVE CASE $\phi \mathcal{R}_I C$: Similar to the above case. □

We show that, depending on which temporal operator is used, by expanding or contracting its interval we can weaken or strengthen the surrounding formula.

Definition 4 (Right-bound modifications of intervals). *Let $I = [a, b]$ be an interval. For any $i \in \mathbb{N}$, a right-bound modification of I is either a right-bound extension $[a, b+i]$, or, provided $i \leq b - a$, a right-bound contraction $[a, b-i]$. A right-bound modification is* strict *if $i > 0$. The set of all right-bound modifications of I is denoted $\mathcal{B}_R(I)$.*

Lemma 5 (Weakening of $\mathcal{U}$ interval). *Let ϕ and ψ be MTL formulae, and I and I' be intervals, where I' is a right-bound extension of I. Then, $\phi \mathcal{U}_I \psi \sqsubseteq \phi \mathcal{U}_{I'} \psi$.*

Proof. We assume that I' is a right-bound extension of I, and so, taking an arbitrary trace π and time-point t, we assume $\pi, t \vDash \phi \mathcal{U}_I \psi$ and want to prove $\pi, t \vDash \phi \mathcal{U}_{I'} \psi$. We know that there exists an $i \in I$ such that $\pi, t+i \vDash \psi$, and that for all $j \in [0, i) \cap I$ we have $\pi, t+j \vDash \phi$. Taking arbitrary i and j, we have that $i, j \in I'$, and so $\pi, t \vDash \phi \mathcal{U}_{I'} \psi$. Thus, $\phi \mathcal{U}_I \psi \sqsubseteq \phi \mathcal{U}_{I'} \psi$. □

Lemma 6 (Weakening of $\mathcal{R}$ interval). *Let ϕ and ψ be MTL formulae, and I and I' be intervals, where I' is a right-bound contraction of I. Then, $\phi \mathcal{R}_I \psi \sqsubseteq \phi \mathcal{R}_{I'} \psi$.*

Proof. We assume that I' is a right-bound contraction of I, and so, taking an arbitrary trace π and time-point t, we assume $\pi, t \vDash \phi \mathcal{R}_I \psi$ and want to prove $\pi, t \vDash \phi \mathcal{R}_{I'} \psi$. By the semantics of $\mathcal{R}$ there are two cases:

1. For all $t' \in I$ we have $\pi, t+t' \vDash \psi$. Then, as $I' \subseteq I$, we know that for all $t'' \in I'$ we have $\pi, t+t' \vDash \psi$, and so $\pi, t \vDash \phi \mathcal{R}_{I'} \psi$.
2. There exists a $t' \in I$ such that $\pi, t+t' \vDash \phi$ and for all $t'' \in I \cap [0, t']$, we have $\pi, t+t'' \vDash \psi$. As I' is a right-bound contraction of I, there are two further cases:
   (a) If $t' \in I'$, then we still have that $\pi, t+t' \vDash \phi$ and for all $t'' \in I' \cap [0, t']$, we have $\pi, t+t'' \vDash \psi$, and so $\pi, t \vDash \phi \mathcal{R}_{I'} \psi$.
   (b) If $t' \notin I'$, then $I' \cap [0, t'] = I'$ and so we know that for all $t'' \in I'$, we have $\pi, t+t'' \vDash \psi$, and so $\pi, t \vDash \phi \mathcal{R}_{I'} \psi$.

Thus, in all cases we have that $\phi \mathcal{R}_I \psi \sqsubseteq \phi \mathcal{R}_{I'} \psi$. □

Often in CEGIW, recursive calls will generate a set of intervals from which either the strongest or weakest must be chosen. We show that there is a total order of implication over the set of right-bound modifications of an interval, which allows us to make that choice.

Lemma 7 (Extension-weakening order of right-bound modifications). *Let I be an interval. Then, $\mathcal{B}_R(I)$ has a total order $\supseteq$, where for all MTL contexts C, MTL formulae ϕ and ϕ', and all $I', I'' \in \mathcal{B}_R(I)$, if $I'' \supseteq I'$ then we have $C[\phi \,\mathcal{U}_{I'}\, \phi'] \sqsubseteq C[\phi \,\mathcal{U}_{I''}\, \phi']$.*

Proof. For any pair of intervals I' and I'' in $\mathcal{B}_R(I)$ we can order the resulting subformulae by applying Lemma 5 to get $\phi \,\mathcal{U}_{I'}\, \phi' \sqsubseteq \phi \,\mathcal{U}_{I''}\, \phi'$ (or the reverse), and then order the full formulae with their contexts by applying Theorem 3 to get $C[\phi \,\mathcal{U}_{I'}\, \phi'] \sqsubseteq C[\phi \,\mathcal{U}_{I''}\, \phi']$ (or the reverse). □

Lemma 8 (Contraction-weakening order of right-bound modifications). *Let I be an interval. Then, $\mathcal{B}_R(I)$ has a total order $\subseteq$, where for all MTL contexts C, MTL formulae ϕ and ϕ', and all $I', I'' \in \mathcal{B}_R(I)$, if $I'' \subseteq I'$ then we have $C[\phi \,\mathcal{R}_{I'}\, \phi'] \sqsubseteq C[\phi \,\mathcal{R}_{I''}\, \phi']$.*

Proof. Similar to the proof of Lemma 7, but uses Lemma 6 to order $\phi \,\mathcal{R}_{I'}\, \phi'$ and $\phi \,\mathcal{R}_{I''}\, \phi'$. □

2 Algorithm for Interval Weakening

CEGIW is split into two levels. First, there is a function *weaken* (Algorithm 1) that, given an MTL formula ϕ, an interval I in ϕ to weaken, and a counterexample trace π, weakens I such that the new formula ϕ' holds on π (Section 2.1). However, this does not guarantee that ϕ' holds on the model itself, and so we need to repeat the process, finding a new counterexample trace for ϕ' and weakening the interval again. The second part of CEGIW is this iterative process that finds counterexample traces by model checking (Section 2.2).

2.1 Weakening on a Counterexample

Model checkers generally produce a specific type of infinite counterexample trace, called a *lasso trace*.

Definition 9 (Lasso traces). *A trace π is* lasso *if it can be separated into a finite prefix π_{pre} and an infinitely repeating finite suffix π_{suf}, forming*

$$\pi = \pi_{\text{pre}}(\pi_{\text{suf}})^{\omega}. \tag{5}$$

This restricts us to a subset of infinite traces that can be finitely represented. The finite length of a lasso trace is then defined as $|\pi| = |\pi_{\text{pre}}| + |\pi_{\text{suf}}|$.

We show that we can prove properties of an entire infinite lasso trace using only a finite *covering interval*. Without this, we may need to iterate over the entire infinite trace, impacting completeness.

Definition 10 (Covering intervals). *The suffix-covering interval of π, defined with respect to an interval $[a, b]$, is*

$$\text{cov}_{\pi}([a, b]) = [a, \min(b, \text{end}_{\pi}(a))] \tag{6}$$

where we specify a finite end *of the infinite trace with*

$$\mathrm{end}_\pi(a) = \begin{cases} |\pi| & \text{if } a < |\pi_{\mathrm{pre}}| \\ a + |\pi_{\mathrm{suf}}| - 1 & \text{otherwise.} \end{cases} \tag{7}$$

Lemma 11 (Lasso trace coverage). *Let ϕ be an MTL formula, π be a lasso trace, and $a \in \mathbb{N}$. If for all $t \in [a, \mathrm{end}_\pi(a)]$ we have $\pi, t \vDash \phi$, then for all $t' \in \mathbb{N}$ with $t' \geq a$ we have $\pi, t' \vDash \phi$.*

Proof. We assume that for all $t \in [a, \mathrm{end}_\pi(a)]$ we have $\pi, t \vDash \phi$, and, taking an arbitrary $t' \in \mathbb{N}$ with $t' \geq a$ want to prove that $\pi, t' \vDash \phi$. There are two cases. Firstly, if $t' < |\pi|$ then we know that this is within the $[a, \mathrm{end}_\pi(a)]$ range and so we have $\pi, t' \vDash \phi$. Otherwise, if $t' \geq |\pi|$, we split π into its prefix π_{pre} and infinitely repeating suffix π_{suf}, and want to prove that $\pi_{\mathrm{pre}}(\pi_{\mathrm{suf}})^\omega, t' \vDash \phi$. As $t' \geq |\pi|$, we can split it into $t' = |\pi_{\mathrm{pre}}| + n \cdot |\pi_{\mathrm{suf}}| + m$ for some $n, m \in \mathbb{N}$ with $n \geq 1$ and $m < |\pi_{\mathrm{suf}}|$.

$$\begin{aligned} & \pi_{\mathrm{pre}}(\pi_{\mathrm{suf}})^\omega, |\pi_{\mathrm{pre}}| + n \cdot |\pi_{\mathrm{suf}}| + m \vDash \phi \\ \implies & (\pi_{\mathrm{suf}})^\omega, n \cdot |\pi_{\mathrm{suf}}| + m \vDash \phi \\ \implies & (\pi_{\mathrm{suf}})^\omega, m \vDash \phi \\ \implies & \pi_{\mathrm{pre}}(\pi_{\mathrm{suf}})^\omega, |\pi_{\mathrm{pre}}| + m \vDash \phi \end{aligned} \tag{8}$$

We know that $|\pi_{\mathrm{pre}}| + m$ is in the $[a, \mathrm{end}_\pi(a)]$ interval, so we have $\pi, t' \vDash \phi$. □

We also define the *optimality* of weakenings, used to prove that CEGIW will not produce an interval weakening that is any stronger than it needs to be.

Definition 12 (Optimality of right-bound extensions and contractions). *An interval I' is an optimal right-bound extension (resp. contraction) of an interval I with respect to a context C, MTL formulae ψ and ψ', a temporal operator $\triangle \in \{\mathcal{U}, \mathcal{R}\}$, trace π, and time-step t, if*

$$\pi, t \vDash C[\psi \triangle_{I'} \psi'] \tag{9}$$

and either (a) $I = I'$, or (b) there exists no strict right-bound contraction (resp. extension) I'' of I' such that $\pi, t \vDash C[\psi \triangle_{I''} \psi']$.

The entrypoint of CEGIW is Algorithm 1, which recurses following the inductive structure of the MTL context grammar. The proof of correctness and optimality follows the same inductive structure, with base cases for directly weakening the intervals of $\mathcal{U}_I$ and $\mathcal{R}_I$ (Lemmas 13 and 14), and inductive cases for weakening within both operators on either side (Lemmas 15 to 18).

Intuitively, to weaken a $\mathcal{U}$ formula $\psi_l \; \mathcal{U}_I \; \psi_r$ in Algorithm 2, the algorithm considers how the interval can be adjusted so that the formula becomes satisfied. Starting from time t, if the formula does not hold under the original interval, the only admissible weakening is to extend the right bound, thereby allowing additional time for the right subformula ψ_r to become true while the left subformula ψ_l continues to hold. The algorithm therefore extends the right bound incrementally until either the $\mathcal{U}$ formula holds on the given trace or no further extension

Algorithm 1: Weakening within a context C

```
1  function Weaken(C, ψ △_{I_orig} ψ', π, t)
2      if C = [−] then
3          if △ = U then
4              return WeakenUDirect(ψ, ψ', I_orig, π, t)
5          else // △ = R
6              return WeakenRDirect(ψ, ψ', I_orig, π, t)
7      ...
8      else if C = C U_J φ then
9          return WeakenULeft(C, φ, J, ψ △_{I_orig} ψ', π, t)
10     else if C = φ U_J C then
11         return WeakenURight(φ, C, J, ψ △_{I_orig} ψ', π, t)
12     else if C = C R_J φ then
13         return WeakenRLeft(C, φ, J, ψ △_{I_orig} ψ', π, t)
14     else if C = φ R_J C then
15         return WeakenRRight(φ, C, J, ψ △_{I_orig} ψ', π, t)
```

Algorithm 2: Directly weakening interval of $\mathcal{U}$

```
1  function WeakenUDirect(ψ_l, ψ_r, [a, b], π, t)
2      for i ← a to end_π(a) do
3          if π, t + i ⊨ ψ_r then
4              return [a, max(b, i)]
5          if π, t + i ⊭ ψ_l then
6              break
7      return None
```

is possible. In the former case, it returns the smallest such extension, yielding an optimal weakening; in the latter case, it reports that no interval weakening exists.

Lemma 13 ($\mathcal{U}$ base case). *Let I be an interval, ψ_l and ψ_r MTL formulae, and π a lasso trace. Then, for all timepoints $t \in \mathbb{N}$ with*

$$I' = WeakenUDirect(\psi_l, \psi_r, I, \pi, t), \tag{10}$$

either I' is an optimal right-bound extension of I such that $\pi, t \vDash \psi_l \, \mathcal{U}_{I'} \, \psi_r$, or $I' = None$, in which case there exists no such interval.

Proof. We take an arbitrary t. Our proof for Algorithm 2 uses the loop invariant that $\forall j \in [a, \text{end}_\pi(a)]$ with $j < i$ (where $I = [a, b]$), we have that $\pi, t+j \nvDash \psi_r$ and $\pi, t+j \vDash \psi_l$. On first entry to the loop there is no such j, so this is trivially true. On reaching the end of the loop body, we know that $\pi, t+i \nvDash \psi_r$ and $\pi, t+i \vDash \psi_l$, and so in combination with the loop invariant we know that $\forall j \in I$ where $j \leq i$, we have $\pi, t + j \nvDash \psi_r$ and $\pi, t + j \vDash \psi_l$. Thus, the loop invariant is preserved. Suppose at the start of iteration i the loop invariant holds. If $\pi, t + j \vDash \psi_r$ on

Algorithm 3: Directly weakening interval of $\mathcal{R}$

```
1  function WeakenRDirect(ψ_l, ψ_r, [a, b], π, t)
2      b_fin ← min(b, end_π(a))
3      for i ← a to b_fin do
4          if π, t + i ⊭ ψ_r then
5              if i = a then
6                  return None
7              return [a, i − 1]
8          if π, t + i ⊨ ψ_l then
9              return [a, b]
10     return [a, b]
```

Algorithm 2 then we return $I' = [a, \max(b, i)]$. This is an optimal right-bound extension of I and we have that $\pi, t \vDash \psi_l \, \mathcal{U}_{I'} \, \psi_r$.

If $None$ is returned, then either we broke out of the loop early because for some $i \in [a, \text{end}_\pi(a)]$ we have $\pi, t + i \nvDash \psi_l$ at Algorithm 2, or we ran the loop to completion. In the first case, we know that $\pi, t + i \nvDash \psi_r$ as this is checked before at Algorithm 2, and so combining with the loop invariant we know that ψ_r never held up until ψ_l stopped holding, and so there is no right-bound extension I' for which $\pi, t \vDash \psi_l \, \mathcal{U}_{I'} \, \psi_r$.

In the second case, by the loop invariant we have that for all $i \in [a, \text{end}_\pi(a)]$ we have $\pi, t + i \vDash \psi_l$ and $\pi, t + i \nvDash \psi_r$. By Lemma 11 we then have the same for all $i \in \mathbb{N}$ with $i \geq a$, and so there exists no right-bound extension I' of I that satisfies $\pi, t \vDash \psi_l \, \mathcal{U}_{I'} \, \psi_r$. □

Lemma 14 ($\mathcal{R}$ base case). *Let I be an interval, ψ_l and ψ_r MTL formulae, and π a lasso trace. Then, for all timepoints $t \in \mathbb{N}$ with*

$$I' = WeakenRDirect(\psi_l, \psi_r, I, \pi, t), \tag{11}$$

either I' is an optimal right-bound contraction of I such that $\pi, t \vDash \psi_l \, \mathcal{R}_{I'} \, \psi_r$, or $I' = None$, in which case there exists no such interval.

Proof. We take an arbitrary t. Our proof for Algorithm 3 uses the loop invariant that for all $j \in \text{cov}_\pi(I)$ with $j < i$, we have that $\pi, t + j \vDash \psi_r$ and $\pi, t + j \nvDash \psi_l$. On first entry to the loop there is no such j, so this is trivially true. On reaching the end of the loop body, we know that $\pi, t + i \nvDash \psi_r$ and $\pi, t + i \vDash \psi_l$, and so in combination with the loop invariant we know that for all $j \in \text{cov}_\pi(I)$ with $j \leq i$, we have that $\pi, t + j \nvDash \psi_r$ and $\pi, t + j \vDash \psi_l$. Thus the loop invariant is preserved. Suppose at the start of iteration i the loop invariant holds. If $\pi, t + i \nvDash \psi_r$ then we have two cases:

1. If $i = a$ we have that $\pi, t + a \nvDash \psi_r$, so for all possible right-bound contractions I' of I we have that $\pi, t \nvDash \psi_l \, \mathcal{R}_{I'} \, \psi_r$. Thus, there is no suitable interval and we return $None$.

2. Otherwise, we return $I' = [a, i-1]$, which is an optimal right contraction of I. By the loop invariant we know for all $j \in \mathrm{cov}_\pi(I)$ with $j < i$ that $\pi, t+j \vDash \psi_r$, so we can conclude that $\pi, t \vDash \psi_l \; \mathcal{R}_{I'} \; \psi_r$.

If during this iteration i we have that $\pi, t+i \vDash \psi_l$, then as this is after the above case is checked for we know that $\pi, t+i \vDash \psi_r$, and in combination with the loop invariant we have that $\pi, t \vDash \psi_l \; \mathcal{R}_I \; \psi_r$. If we run the loop to completion, then by the loop invariant we know that for all $i \in \mathrm{cov}_\pi(I)$ we have $\pi, t+j \vDash \psi_r$. If $\mathrm{cov}_\pi(I) = I$ then we have

$$\pi, t \vDash \psi_l \; \mathcal{R}_I \; \psi_r$$

If $\mathrm{cov}_\pi(I) = [a, \mathrm{end}_\pi(a)]$ for some $a \in \mathbb{N}$, then by Lemma 11 we have that for all $i \in \mathbb{N}$ with $i \geq a$ we have $\pi, t+j \vDash \psi_r$, and so the above holds here too. □

We prove the inductive cases with an MTL context C, an interval I, MTL formulae ψ and ψ', a temporal operator $\triangle \in \{\mathcal{U}, \mathcal{R}\}$, and a lasso trace π. We use the induction hypothesis $P(C)$, that for all timepoints $t \in \mathbb{N}$ with $I' = Weaken(C, \psi \triangle_I \psi', \pi, t)$, if I' is an interval then $\pi, t \vDash C[\psi \triangle_I \psi']$, and

1. If $\triangle = \mathcal{U}$, then I' is an optimal right-bound extension of I;
2. If $\triangle = \mathcal{R}$, then I' is an optimal right-bound contraction of I.

If $I' = None$, then there exists no such interval in each case.

Intuitively, when weakening within the left subformula of a $\mathcal{U}$ operator in Algorithm 4, we must ensure that the left subformula holds at every relevant timestep until the right subformula becomes true. Starting from time t, the algorithm therefore examines each timestep $t+i$ within the original interval and determines the interval weakening required for the left subformula to hold on the given trace at that point. Because the left operand of $\mathcal{U}$ is interpreted universally over the interval, the overall weakening must be strong enough to satisfy all such requirements. The algorithm therefore selects the weakest interval that subsumes all interval weakenings computed for individual timesteps. If no such interval exists, or if weakening fails at any timestep, the algorithm reports that no valid weakening can be found.

Lemma 15 ($\mathcal{U}$-left inductive case). *Let C be an MTL context, I and J intervals, ϕ, ψ, and ψ' MTL formulae, $\triangle \in \{\mathcal{U}, \mathcal{R}\}$ a temporal operator, and π a lasso trace. If $P(C)$ holds, then so does $P(C \; \mathcal{U}_J \; \phi)$.*

Proof. For Algorithm 4 we assume the inductive hypothesis $P(C)$ and want to prove $P(C \; \mathcal{U}_J \; \phi)$. We take an arbitrary t and distinguish two cases, according to whether $\triangle$ is $\mathcal{U}$ or $\mathcal{R}$. In either case, by the induction hypothesis each recursive call evaluates to either $None$ or an optimal interval I' related to I by the corresponding relation (right-bound extension or contraction respectively) such that $\pi, t+t' \vDash C[\psi \triangle_{I'} \psi']$.

We use the loop invariant that, for all $j \in \mathrm{cov}_\pi(J)$ with $j < i$, we have that $\pi, t+j \nvDash \phi$ and that $I' = Weaken(C, \psi \triangle_I \psi', \pi, t+j)$ is an interval such that $\pi, t+j \vDash C[\psi \triangle_{I'} \psi']$. On first entry to the loop there is no such j, so this is trivially true. On reaching the end of the loop body, we know

Algorithm 4: Weakening within $\mathcal{U}$ on the left

```
1  function WeakenULeft(C, φ, [a, b], ψ △_{I_orig} ψ', π, t)
2      b_fin ← min(b, end_π(a))
3      intervals ← [ ]
4      for i ← a to b_fin do
5          if π, t + i ⊨ φ then
6              if i = a then
7                  return I_orig
8              return interval in intervals with maximal absolute difference to
                   I_orig
9          I ← Weaken(C, ψ △_{I_orig} ψ', π, t + i)
10         if I = None then
11             return None
12         append I to intervals
13     return None
```

that $Weaken(C, \psi \triangle_I \psi', \pi, t + i) \neq None$ from Algorithm 4, and so by the induction hypothesis the recursive call must have produced a suitable interval I'. As we also know that $\pi, t + i \not\models \phi$ from Algorithm 4, the loop invariant is thus preserved for $j \leq i$. Suppose at the start of iteration i the loop invariant holds. If $Weaken(C, \psi \triangle_I \psi', \pi, t + i) = None$ at Algorithm 4 then by the induction hypothesis we know that there is no suitable interval I'' for which $\pi, t + i \models C[\psi \triangle_{I''} \psi']$, and by the loop invariant that there is no $j < i$ for which $\pi, t + j \models \phi$. Thus, there is no suitable interval I'' for which $\pi, t \models (C \,\mathcal{U}_J\, \phi)[\psi \triangle_{I''} \psi']$. If $\pi, t + j \models \phi$ at Algorithm 4 then we split on whether it is our first iteration or not. If $i = a$ (where $J = [a, b]$) then we know that $\pi, t + a \models \phi$, and so any interval will work. We simply return the original interval I_{orig}.

Otherwise, by the loop invariant we know that for all $j \in \text{cov}_\pi(J)$ with $j < i$ — of which there must be at least one as $i > a$ — we have an interval I' such that $\pi, t + j \models C[\psi \triangle_{I'} \psi']$. Applying Lemma 7 if $\triangle = \mathcal{U}$, or Lemma 8 if $\triangle = \mathcal{R}$, we obtain a maximum interval I'' such that for all $j \in \text{cov}_\pi(J)$ with $j < i$ we have $\pi, t + j \models C[\psi \triangle_{I''} \psi']$. If $\text{cov}_\pi(J) = J$ then we have

$$\pi, t \models (C \,\mathcal{U}_J\, \phi)[\psi \triangle_{I''} \psi']. \tag{12}$$

Otherwise, if $\text{cov}_\pi(J) = [a, \text{end}_\pi(a)]$, then by Lemma 11 for all $k \in \mathbb{N}$ with $k \geq a$ we have $\pi, t + k \models C[\psi \triangle_{I''} \psi']$, and so the above holds here too. □

Lemma 16 ($\mathcal{U}$-right inductive case). *Let C be an MTL context, I and J intervals, ϕ, ψ, and ψ' MTL formulae, $\triangle \in \{\mathcal{U}, \mathcal{R}\}$ a temporal operator, and π a lasso trace. If $P(C)$ holds, then so does $P(\phi \,\mathcal{U}_J\, C)$.*

Proof. We assume the inductive hypothesis $P(C)$, and want to prove $P(\phi \,\mathcal{U}_J\, C)$. We take an arbitrary t. We distinguish two cases, according to whether $\triangle$ is $\mathcal{U}$

Algorithm 5: Weakening within $\mathcal{U}$ on the right

```
function WeakenURight(C, φ, [a, b], ψ △_{I_orig} ψ', π, t)
    b_fin ← min(b, end_π(a))
    intervals ← [ ]
    for i ← a to b_fin do
        I ← Weaken(C, ψ △_{I_orig} ψ', π, t + i)
        if I ≠ None then
            append I to intervals
        if π, t + i ⊭ φ then
            break
    if intervals is empty then
        return None
    return interval in intervals with minimal absolute difference to I_orig
```

or $\mathcal{R}$. In either case, by the induction hypothesis each recursive call evaluates to either *None* or an interval I' related to I by the corresponding relation (right-bound extension or contraction respectively) such that $\pi, t + t' \vDash C[\psi \triangle_{I'} \psi']$.

We use the loop invariant that for all $j \in \mathrm{cov}_\pi(J)$ with $j < i$, we have that $\pi, t + j \vDash \phi$. On first entry to the loop there is no such j, so this is trivially true. On reaching the end of the loop body, we know for all $j \in \mathrm{cov}_\pi(J)$ with $j \leq i$ that $\pi, t + j \vDash \phi$, and so the loop invariant is preserved. Suppose at the start of iteration i the loop invariant holds. If $\pi, t + i \nvDash \phi$ we exit the loop, and if the list of intervals is empty then by the loop invariant we know that there are no appropriate intervals I' for any $j \in \mathrm{cov}_\pi(J)$ with $j < i$ for which $\pi, t + j \vDash C[\psi \triangle_{I'} \psi']$, and so the same holds for $\pi, t \vDash (\phi \,\mathcal{U}_J\, C)[\psi \triangle_{I'} \psi']$.

Otherwise, by the loop invariant we know that for all $j \in \mathrm{cov}_\pi(J)$ with $j < i$ we have $\pi, t + j \vDash \phi$ and, as we have passed the check above, that for at least one of these j we have an interval I' such that $\pi, t + j \vDash C[\psi \triangle_{I'} \psi']$. Thus, we have

$$\pi, t \vDash (\phi \,\mathcal{U}_J\, C)[\psi \triangle_{I'} \psi']$$

□

Lemma 17 ($\mathcal{R}$-left inductive case). *Let C be an MTL context, I and J intervals, ϕ, ψ, and ψ' MTL formulae, $\triangle \in \{\mathcal{U}, \mathcal{R}\}$ a temporal operator, and π a lasso trace. If $P(C)$ holds, then so does $P(C \,\mathcal{R}_J\, \phi)$.*

Proof. We assume the inductive hypothesis $P(C)$, and want to prove $P(\phi \,\mathcal{R}_J\, C)$. We take an arbitrary t. We distinguish two cases, according to whether $\triangle$ is $\mathcal{U}$ or $\mathcal{R}$. In either case, by the induction hypothesis each recursive call evaluates to either *None* or an interval I' related to I by the corresponding relation (right-bound extension or contraction respectively) such that $\pi, t + t' \vDash C[\psi \triangle_{I'} \psi']$.

We use the loop invariant that for all $j \in \mathrm{cov}_\pi(J)$ with $j < i$, we have that $\pi, t + j \nvDash \phi$ and that $I' = \mathit{Weaken}(C, \psi \triangle_I \psi', \pi, t + j)$ is an interval

Algorithm 6: Weakening within $\mathcal{R}$ on the left

```
1  function WeakenRLeft(C, φ, [a,b], ψ △_{I_orig} ψ', π, t)
2      b_fin ← min(b, end_π(a))
3      intervals ← [ ]
4      for i ← a to b_fin do
5          if π, t+i ⊭ φ then
6              break
7          I ← Weaken(C, ψ △_{I_orig} ψ', π, t+i)
8          if I ≠ None then
9              append I to intervals
10     if intervals is empty then
11         return None
12     return interval in intervals with minimal absolute difference to I_orig
```

such that $\pi, t + j \vDash C[\psi \triangle_{I'} \psi']$. On first entry to the loop there is no such j, so this is trivially true. On reaching the end of the loop body, we know that $Weaken(C, \psi \triangle_I \psi', \pi, t + i) \neq None$, and so by the induction hypothesis the recursive call must have produced a suitable interval I'. As we also know that $\pi, t + i \nvDash \phi$, the loop invariant is thus preserved for $j \in \mathrm{cov}_\pi(J)$ with $j \leq i$. Suppose at the start of iteration i the loop invariant holds. If $I' = Weaken(C, \psi \triangle_I \psi', \pi, t + i) = None$ then by the induction hypothesis we know that there is no suitable interval I'' for which $\pi, t + i \vDash C[\psi \triangle_{I''} \psi']$, and by the loop invariant that there is no $j \in \mathrm{cov}_\pi(J)$ with $j < i$ for which $\pi, t + j \vDash \phi$. Thus, there is no interval I'' for which $\pi, t \vDash (C \,\mathcal{U}_J\, \phi)[\psi \triangle_{I''} \psi']$.

If $\pi, t+i \vDash \phi$, then we exit the loop. As this check occurred after the recursive call to $Weaken$, we know that we have found at least one suitable interval. By the loop invariant we know that for all $j \in \mathrm{cov}_\pi(J)$ with $j < i$ we have an interval I' such that $\pi, t + j \vDash C[\psi \triangle_{I'} \psi']$. Applying Lemma 7 if $\triangle = \mathcal{U}$, or Lemma 8 if $\triangle = \mathcal{R}$, we obtain a maximum interval I'' such that for all $j \in \mathrm{cov}_\pi(J)$ with $j \leq i$ we have $\pi, t + j \vDash C[\psi \triangle_{I''} \psi']$, and so

$$\pi, t \vDash (\phi \,\mathcal{R}_J\, C)[\psi \triangle_{I''} \psi']$$

If we run the loop to completion, then by the loop invariant for each $i \in \mathrm{cov}_\pi(J)$ we have a suitable interval I' where $\pi, t + j \vDash C[\psi \triangle_{I'} \psi']$. If $\mathrm{cov}_\pi(J) = J$ then by the same reasoning as above we have a suitable maximum interval. If $\mathrm{cov}_\pi(J) = [a, \mathrm{end}_\pi(a)]$ for some a then by Lemma 11 this property holds for all $i \in \mathbb{N}$ with $i \geq a$, and so in this case we also have a maximum interval. □

Lemma 18 ($\mathcal{R}$-right inductive case). *Let C be an MTL context, I and J intervals, ϕ, ψ, and ψ' MTL formulae, $\triangle \in \{\mathcal{U}, \mathcal{R}\}$ a temporal operator, and π a lasso trace. If $P(C)$ holds, then so does $P(\phi \,\mathcal{R}_J\, C)$.*

Proof. We assume the inductive hypothesis $P(C)$, and want to prove $P(C \,\mathcal{R}_J\, \phi)$. We take an arbitrary t. We distinguish two cases, according to whether $\triangle$ is $\mathcal{U}$

Algorithm 7: Weakening within $\mathcal{R}$ on the right

```
1  function WeakenRRight(C, φ, [a, b], ψ △_{I_orig} ψ', π, t)
2      b_fin ← min(b, end_π(a))
3      intervals ← [ ]
4      for i ← a to b_fin do
5          I ← Weaken(C, ψ △_{I_orig} ψ', π, t + i)
6          if I = None then
7              return None
8          append I to intervals
9          if π, t + i ⊨ φ then
10             break
11     return interval in intervals with maximal absolute difference to I_orig
```

or $\mathcal{R}$. In either case, by the induction hypothesis each recursive call evaluates to either $None$ or an interval I' related to I by the corresponding relation (right-bound extension or contraction respectively) such that $\pi, t + t' \vDash C[\psi \triangle_{I'} \psi']$.

We use the loop invariant that for all $j \in \mathrm{cov}_\pi(J)$ with $j < i$, we have that $\pi, t + j \vDash \phi$. On first entry to the loop there is no such j, so this is trivially true. On reaching the end of the loop body, we know that for all $j \in \mathrm{cov}_\pi(J)$ with $j \leq i$ that $\pi, t + j \vDash \phi$, so the loop invariant holds. Suppose at the start of iteration i the loop invariant holds. If $\pi, t + i \nvDash \phi$ we exit the loop, and if the list of intervals is empty then we know that there are no appropriate intervals I' for any $j \in \mathrm{cov}_\pi(J)$ with $j < i$ for which $\pi, t + j \vDash C[\psi \triangle_{I'} \psi']$, and so the same holds for $\pi, t \vDash (C \mathcal{R}_J \phi)[\psi \triangle_{I'} \psi']$.

Otherwise, by the loop invariant we know that for all $j \in \mathrm{cov}_\pi(J)$ with $j < i$ we have $\pi, t + j \vDash \phi$, and, as we have passed the check above, that for at least one of these j we have an interval I' such that $\pi, t + j \vDash C[\psi \triangle_{I'} \psi']$. Thus, we have

$$\pi, t \vDash (C \mathcal{R}_J \phi)[\psi \triangle_{I'} \psi']$$

□

We use these supporting lemmas to prove the correctness and optimality of CEGIW.

Theorem 19 (Correctness for weakening). *Let C be an MTL context, I and J intervals, ϕ, ψ, and ψ' MTL formulae, $\triangle \in \{\mathcal{U}, \mathcal{R}\}$ a temporal operator, π a lasso trace, and $t \in \mathbb{N}$ be a timepoint. Let $I' = Weaken(C, \psi \triangle_I \psi', \pi, t)$. If I' is an interval then $\pi \vDash C[\psi \triangle_{I'} \psi']$, and*

1. *If $\triangle = \mathcal{U}$, then I' is an optimal right-bound extension of I;*
2. *If $\triangle = \mathcal{R}$, then I' is an optimal right-bound contraction of I.*

If $I' = None$, then there exists no such interval in each case.

Proof. We use the same induction hypothesis $P(C)$ defined for the preceding inductive lemmas. The non-temporal inductive cases are omitted for brevity.

BASE CASE $[-]$: By Lemma 13 if $\triangle = \mathcal{U}$, and Lemma 14 if $\triangle = \mathcal{R}$, we have $P([-])$.
INDUCTIVE CASE $C\,\mathcal{U}_J\,\phi$: Assuming $P(C)$, by Lemma 15 we have $P(C\,\mathcal{U}_J\,\phi)$.
INDUCTIVE CASE $\phi\,\mathcal{U}_J\,C$: Assuming $P(C)$, by Lemma 16 we have $P(\phi\,\mathcal{U}_J\,C)$.
INDUCTIVE CASE $C\,\mathcal{R}_J\,\phi$: Assuming $P(C)$, by Lemma 17 we have $P(C\,\mathcal{R}_J\,\phi)$.
INDUCTIVE CASE $\phi\,\mathcal{R}_J\,C$: Assuming $P(C)$, by Lemma 18 we have $P(\phi\,\mathcal{R}_J\,C)$.
□

The time complexity of Algorithm 1 is $O(|\pi|^{\mathtt{td}(\phi)})$. where π is the counterexample trace and $\mathtt{td}(\phi)$ is the *temporal depth* of the MTL formula ϕ, i.e. the maximum number of nested temporal operators along any path in the syntax tree.

2.2 Iterative Weakening

Assume that we have an MTL formula ϕ that has a temporal subformula $\psi \triangle_I \psi'$ with an interval I that we want to weaken. ϕ can be split into $\psi \triangle_I \psi'$ and the surrounding MTL context C, such that ϕ is logically equivalent to $C[\psi \triangle_I \psi']$. Assume we also have a transition system $\mathcal{M}$. Using a model checker, we check whether ϕ holds on $\mathcal{M}$. If it holds then we are done, but if not, we will receive a counterexample trace π through $\mathcal{M}$ for which $\pi \not\models C[\psi \triangle_I \psi']$. We can then weaken on this counterexample with

$$I' = Weaken(C, \psi \triangle_I \psi', \pi, 0). \tag{13}$$

By Theorem 19, if $I' = None$, then there exists no weakening I'' of I such that $\pi \vDash C[\psi \triangle_{I''} \psi']$, and so the same holds for the model $\mathcal{M}$. Otherwise, I' is an interval such that $\pi \vDash C[\psi \triangle_{I'} \psi']$. However, $C[\psi \triangle_{I'} \psi']$ does not necessarily hold on $\mathcal{M}$, and so we model check again, creating an iterative loop that ends when we either produce an interval I'' that is a weakening of I such that $C[\psi \triangle_{I''} \psi']$ holds on $\mathcal{M}$, or show that no such weakening exists.

References

[1] R. Alur and T. A. Henzinger. "Real-Time Logics: Complexity and Expressiveness". In: *Information and Computation* 104.1 (1993).
[2] R. Koymans. "Specifying Real-Time Properties with Metric Temporal Logic". In: *Real-Time Systems* 2.4 (1990).