Corrigenda: On the Complexity of Modal Logic Variants and their Fragments

Arne Meier

May 8, 2018

"Love truth, but pardon error." — Voltaire

This corrigenda corrects some errors from my dissertation *Arne Meier, On the Complexity of Modal Logic Variants and their Fragments, Gottfried Wilhelm Leibniz Universität Hannover, Cuvillier Verlag, 2011.*

Proof of Theorem 1 (1): The result is correct but the proof is wrong. It is not possible to simulate $\top$ as by Lewis [4] done without preventing an exponential blow up. There are no (wrongly assumed) short representations of $\wedge$ in S_1 available. Yet the result of Theorem 1 (1) is still valid. Lück [5, Lemma 5.1, Theorem 6.1] has shown that the lower bounds already hold for temporal depth of 2. Hence the reduction mentioned by us works in that case as we only have two subformulas (due to nesting depth of 2) where we need to add $\wedge t$ and the non-existence of short representations does thus not matter as the blowup in the length of the formula is only of constant size.

Theorem 3.4 (1), Lemma 3.5: The result and the proof are wrong. Therefore consider a formula of the form $\phi = \mathsf{AF}(p_1 \wedge \cdots \wedge p_n)$ together with a Kripke structure $M = (W, R, \eta)$ of the form $W = \{w_0, \ldots, w_{2^n}\}$, $R = \{\, (w_i, w_{i+1}) \mid 1 \leq i \leq 2^n - 1 \,\}$, and $\eta(w_i) = \{\, p_j \mid \text{the } j\text{th bit in the binary representation of } i \text{ is true} \,\}$. In the proof a modification of Emerson quotient construction [1] is investigated. However the problem with this model M is its so to speak distinctness. For each world there is a different quasi label wherefore the model produced from the quotient construction will stay the same and hence will not be of size polynomial in $|\phi|$ and the number of temporal operators in ϕ.

This fragment is not NP-complete but PSPACE-complete instead. Lück [5, Theorem 3.4] instead shows how to encode validity of quantified Boolean formulas into formulas of this kind. By this reduction there are exponentially long paths in the models wherefore these models cannot be guessed (as they are too large) and invalidate the Claim in Lemma 3.5.

Theorem 3.4 (2) PSPACE membership {AF, AG}, Lemma 3.6: Both, the result and the proof are wrong. The membership proof assumes the existence of quasi-models in which possible contradictions must occur in at most linear depth. The induction proof wrongly assumes that in the case of $\psi \wedge \chi$ minimal quasi models of both ψ and χ are always contained in the model of $\psi \wedge \chi$. Now Lück [5, Theorem 3.18 (2)] shows that it is possible to encode exponentially deep paths into the model leading to an EXP lower bound instead contradicting the PSPACE upper bound (under reasonable complexity separation assumptions).

Theorem 3.4 (2) PSPACE membership {AX, AF}, Lemma 3.6: The result is correct but the proof is wrong. On page 37, line -5, it is claimed that an {AFAX}-formula is satisfiable iff it is satisfiable with EG (resp., ¬AF) operators ignored and each EG-preceded subformula is satisfiable on its own. This does not work in general as the duality of EG and AF has been neglected. Yet the PSPACE upper bound result is still valid as shown by Lück [5, Theorem 3.17] via a different algorithm.

Theorem 3.4 (3) EXP lower bound {AU}, Lemma 3.7 The result is correct but the proof is wrong. The end of the proof it claims "Finally, φ_3 stat:es that, on *all* paths, the contents of all tape cells remains unchanged *until* either the head moves onto the cell or π_{term} holds." A direct translation of this informally given requirement to a linear number of AU subformulas would lead to an incorrect reduction. However the result is still valid and Lück [5, Theorem 3.18 (3)] shows that our reduction can be slightly modified to circumvent this problem.

Theorem 3.9 (2): Several PSPACE upper bounds for CTL*-SAT are claimed with quite a vague comment that they can be proven similar as for the CTL-cases. While this is true for the {A, X} case, now we instead know EXP-hardness for the {A, F} fragment from the corrections of CTL-SAT({AF}) which is now lacks a matching upper bound.

Theorem 3.10 (2): The result and the proof is wrong. Follows from the corrections of CTL-SAT({AF}).

Corollary 3.13 (2): The result and the proof is wrong. Follows from the corrections of CTL-SAT({AF}). Only PSPACE-hardness is known.

Theorem 3.14: Here, only PSPACE-hardness can be shown. Follows from the corrections of CTL-SAT({AF}).

The errors with respect to the CTL-SAT and CTL*-SAT cases are also present in the corresponding journal publication "Arne Meier, Martin Mundhenk, Michael Thomas, Heribert Vollmer: *The Complexity of Satisfiability for Fragments of CTL and CTL**, International Journal of Foundations of Computer Science, Vol. 20, No. 5, pp. 901—918, 2009" and have been already corrected and published in the erratum "Arne Meier, Martin Mundhenk, Michael Thomas, Heribert Vollmer: *Erratum: The Complexity of Satisfiability for Fragments of CTL and CTL**, International Journal of Foundations of Computer Science, Vol. 26, No. 08, pp. 1189—1190, 2015".

Base independence for BF

For sake of completeness we state a construction which shows all necessary technical details to prove base independence for the clone BF. The reduction follows the approach of Hemaspaandra et al. [3, Theorem 3.6].

Theorem 1. *Let B be a finite set of Boolean functions such that $[B] = \mathsf{BF}$, and let $\mathcal{T} \subseteq \{\mathsf{A}, \mathsf{E}, \mathsf{X}, \mathsf{F}, \mathsf{G}, \mathsf{U}\}$. Then it holds that*

$$\text{CTL}^\star\text{-SAT}(\mathcal{T}, B) \leq_m^{log} \text{CTL}^\star\text{-SAT}(\mathcal{T}, \{\wedge, \vee, \neg\}).$$

Proof. The proof makes use of temporal circuits, the temporal logic variant of modal circuits defined in [3]. Note that this kind of circuits is just a syntactic variant of a graphical way to present formulas in a succinct way. A *temporal circuit* over the basis B and set of operators $\mathcal{T}$ is a tuple $X = (G, I, E, \alpha, \beta, \mathsf{out})$, where

- (G, E) is a finite directed acyclic graph with G being the set of gates,
- $I \subseteq G$ being the set of input gates
- $\alpha : E \to \mathbb{N}$ is an injective function which defines an ordering on the edges and thereby on the children of a gate,
- $\beta : G \to B \cup \mathcal{T}$ is a function assigning a Boolean function, or a temporal operator to every gate such that $\beta(g) \in \mathsf{PROP}$ iff $g \in I$,and
- $\mathsf{out} \in G$, the *output gate*,

and the following conditions are satisfied.

- If $g \in G$ has in-degree 0, then $\beta(g)$ is an atomic concept or one of the constants $\top, \bot$ (if they are in $[B]$).
- If $g \in G$ has in-degree 1, then $\beta(g)$ is a unary Boolean function from B or some unary temporal operator $T \in \{\mathsf{A}, \mathsf{E}, \mathsf{X}, \mathsf{F}, \mathsf{G}\}$.
- If $g \in G$ has in-degree 2, then $\beta(g)$ is a binary Boolean function from B or the temporal operator until U.
- If $g \in G$ has in-degree $d > 2$, then $\beta(g)$ is a d-ary Boolean function from B.

The function α is needed to define the order of arguments of non-symmetric functions. The *size* of a temporal circuit is the number of its gates.

Every formula φ can straightforwardly be transformed into a temporal circuit of linear size that resembles the ordered tree induced by φ. For the backward transformation, an exponential blowup may occur if the circuit is not tree-shaped.

In order to establish the reduction $\text{CTL}^\star\text{-SAT}(\mathcal{T}, B) \leq_m^{\log} \text{CTL}^\star\text{-SAT}(\mathcal{T}, \mathsf{BF})$, we proceed analogously to [3] and translate, for any given instance φ of $\text{CTL}^\star\text{-SAT}(\mathcal{T}, B)$, the formula into a temporal circuit X_φ over the basis B and temporal operator set

$\mathcal{T}$. This circuit can be easily transformed into a circuit X'_φ over the basis $\{\wedge, \vee, \neg\}$ by replacing every $\circ$-gate, for $\circ \in B$, with a sub-circuit over $\{\wedge, \vee, \neg\}$. This replacement is possible because of $[B] = \mathsf{BF}$. Further it causes only linear blowup because the size of the sub-circuits is bounded by a constant. However, since the sub-circuits may not be tree-shaped, we cannot directly transform X'_φ back to a formula over $\{\wedge, \vee, \neg\}$ and $\mathcal{T}$ without exponential blowup. Instead, we will express the circuit X'_φ with a new formula $f(C, \varphi)$ which is build from subformulas that model the gates from X'_φ:

- For input gates $g \in I$, we define $f'(g) := g \leftrightarrow x_i$.
- If g is a gate computing the Boolean operator $\circ$ for some function in B and $h_1, \ldots, h_n$ are the respective predecessor gates in this circuit, we define $f'(g) := g \leftrightarrow \circ(h_1, \ldots, h_n)$.
- If $T \in \mathcal{T}$ is a unary temporal operator and h its predecessor gate in the circuit, we define $f'(g) := g \leftrightarrow Th$.
- If $T = \mathsf{U}$ is an until operator and h_1, h_2 its predecessor gates in the circuit, we define $f'(g) := g \leftrightarrow h_1 \mathsf{U} h_2$.

Here $\varphi \leftrightarrow \psi$ is a shorthand for $(\neg\varphi \wedge \neg\psi) \vee (\varphi \wedge \psi)$. Finally the formula $f(C, \varphi)$ is defined as

$$f(C,\varphi) := \mathsf{out} \wedge \bigwedge_{\text{gate } g \text{ in } C} \begin{cases} \mathsf{G} f'(C,g) & , \text{ if } \{\mathsf{G},\mathsf{F},\mathsf{U}\} \cap \mathcal{T} \neq \emptyset, \\ \bigwedge_{i=0}^{\mathrm{md}(\varphi)} \mathsf{X}^i f'(C,g) & , \text{ if } \{\mathsf{G},\mathsf{F},\mathsf{U}\} \cap \mathcal{T} = \emptyset \text{ and } \mathsf{X} \in \mathcal{T}, \\ f'(C,g) & , \text{ otherwise.} \end{cases}$$

Note that $\leftrightarrow$ is not nested in $f(C, \varphi)$. This reduction is computable in logarithmic space: (1) create the temporal circuit X_φ (two binary counters for correct bracketing, one counter for position), (2) create translated circuit X'_φ (local substitutions of constant depth), (3) create $f(X'_\varphi, \varphi)$ (binary counter for position in circuit, binary counter for modal depth of φ). The correctness can be shown in the same way as in the proof of [3]. □

Corollary 1. *Let B be a finite set of Boolean functions such that $[B] = \mathsf{BF}$, and let $\mathcal{T} \subseteq \{\, PT \mid P \in \{\mathsf{A}, \mathsf{E}\}, T \in \{\mathsf{F}, \mathsf{G}, \mathsf{X}, \mathsf{U}\} \,\}$. Then it holds that*

$$CTL\text{-SAT}(\mathcal{T}, B) \leq_m^{log} CTL\text{-SAT}(\mathcal{T} \cup \{\mathsf{AG}\}, \{\wedge, \vee, \neg\}).$$

Proof. Redefine the function f as follows

$$f(C,\varphi) := \mathsf{out} \wedge \bigwedge_{\text{gate } g \text{ in } C} \mathsf{AG} f'(C,g).$$

□

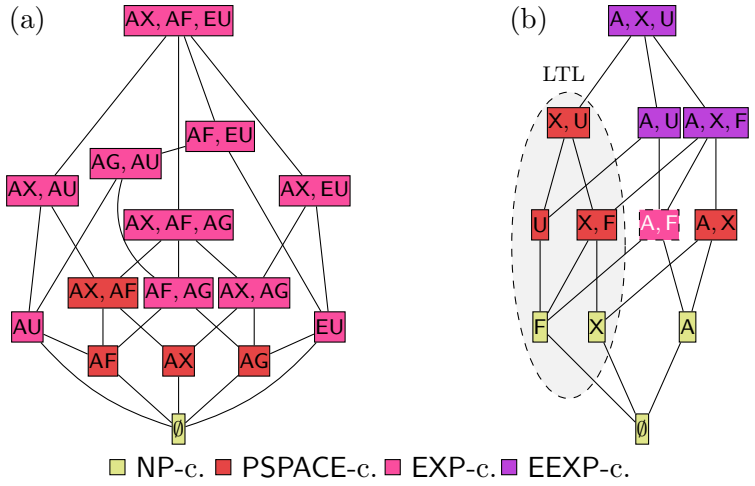

Figure 1: The complexity of (a) CTL-SAT(T, BF), and (b) CTL*-SAT(T, BF), all without any restrictions to the Boolean functions. White coloured text and the dashed borders indicate hardness result.

From Theorem 1 and Corollary 1 we achieve the corresponding complexity results generalised to BF and the mentioned fragments. Now, in essence, there is one case left: $\{\mathsf{AX}, \mathsf{AF}\}$. Here, CTL-SAT($B$, $\{\mathsf{AF}, \mathsf{AX}\}$) is in PSPACE for $B = \{\wedge, \vee, \neg\}$ [5, Theorem 3.17] and the algorithm can be adjusted as follows. For arbitrary B with $[B] = \mathsf{BF}$ the presented algorithm is easily adopted to work for arbitrary bases as the relevant line 11 in the algorithm just talks about violation of quasi-label conditions which does not stick to the allowed Boolean functions. Hence all presented cases are now generalised to BF.

Figure 1 then depicts the corrected landscape of the computational complexity of the satisfiability problems for CTL and CTL* for all temporal fragments and the base BF.

Acknowledgements

I am very thankful to Martin Lück who cleverly spotted these errors and even was able to present several corrections by himself [5].

References

[1] E. Allen Emerson, *Temporal and Modal Logic*, Chapter 16 in Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics, 1994.

[2] E. Allen Emerson, J. Y. Halpern, *Decision Procedures and Expressiveness in the Temporal Logic of Branching Time*, Journal of Comp. and Syst. Sc., **30**, No. 1, 1985.

[3] E. Hemaspaandra, H. Schnoor, I. Schnoor, *Generalized modal satisfiability*, Journal of Computer and System Sciences, **76**, No. 7, pp. 561–578, 2010.

[4] H. Lewis, *Satisfiability problems for propositional calculi*, Math. Sys. Theory, **13**, pp. 45–53, 1979.

[5] M. Lück, *Quirky Quantifiers: Optimal Models and Complexity of Computation Tree Logic*, Int. J. Found. Comput. Sci., **29**, 17, pp. 17–61, 2018, https://doi.org/10.1142/S0129054118500028.

[6] A. Meier, M. Mundhenk, M. Thomas, H. Vollmer: *The Complexity of Satisfiability for Fragments of CTL and CTL⋆*, International Journal of Foundations of Computer Science, Vol. 20, No. 5, pp. 901—918, 2009.

[7] A. Meier, M. Mundhenk, M. Thomas, H. Vollmer: *Erratum: The Complexity of Satisfiability for Fragments of CTL and CTL⋆*, International Journal of Foundations of Computer Science, Vol. 26, No. 08, pp. 1189—1190, 2015