The Second Order Traffic Fine: Temporal Reasoning in European Transport Regulations

Ana de Almeida Borges
University of Barcelona, Spain
anadealmeidagabriel@ub.edu

Juan José Conejero Rodríguez
University of Barcelona, Spain
juan.conejero@ub.edu

David Fernández-Duque[1]
Ghent University, Belgium
David.FernandezDuque@Ugent.be

Mireia González Bedmar
University of Barcelona, Spain
m.gonzalezbedmar@ub.edu

Joost J. Joosten
University of Barcelona, Spain
jjoosten@ub.edu

Abstract

We argue that European transport regulations can be formalized within the Σ^1_1 fragment of monadic second order logic, and possibly weaker fragments including linear temporal logic. We consider several articles in the regulation to verify these claims.

2012 ACM Subject Classification Theory of computation → Modal and temporal logics; Theory of computation → Higher order logic; Applied computing → Law

Keywords and phrases linear temporal logic, monadic second order logic, formalized law, transport regulations

Digital Object Identifier 10.4230/LIPIcs.TIME.2019.6

Funding *Ana de Almeida Borges*: 2016 DI 032, Generalitat de Catalunya, Departament d'Empresa i Coneixement
Juan José Conejero Rodríguez: RTC-2017-6740-7, Spanish Ministry of Science and Universities
David Fernández-Duque: RTC-2017-6740-7, Spanish Ministry of Science and Universities
Mireia González Bedmar: RTC-2017-6740-7, Spanish Ministry of Science and Universities
Joost J. Joosten: RTC-2017-6740-7, Spanish Ministry of Science and Universities; 2016 DI 032 and 2016 DI 033, Generalitat de Catalunya, Departament d'Empresa i Coneixement; SGR 270, Generallitat de Catalunya; FFI2015-70707P, Spanish Ministry of Economy and Competitiveness

Acknowledgements We are grateful to Albert Atserias and Martín Diéguez for insightful discussions involving Kamp's theorem and its variants.

1 Introduction

The authors of the paper are involved in research projects that collaborate with industry, lawyers and legislators where the main goal is to develop verified legal software. The industrial and social need is evident: various legal decisions are made on the basis of

[1] Corresponding author

26th International Symposium on Temporal Representation and Reasoning (TIME 2019).
Editors: Johann Gamper, Sophie Pinchinat, and Guido Sciavicco; Article No. 6; pp. 6:1–6:16
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

algorithmic processing of data in consequence of which individuals can be fined or even sent to jail. Software contains errors, but for our legal context such errors should not be acceptable.

In particular, the above-mentioned projects have as first and main objective to eradicate errors from software that interprets data from tachographs. A tachograph is to a truck what a black-box is to an aeroplane: it registers all kinds of activities from the truck and driver, like speed, movement and others. In practice, a police officer may pull over a truck for an inspection where the tachograph data is read and interpreted by some software. Depending on the verdict of the program, the driver may be instantly fined or sometimes even imprisoned. It is known that many erroneous automated verdicts are issued. This is highly undesirable both from an industrial and from a civil rights perspective. It is here that logic tries to come to the rescue.

The aim of the project is to recast the transport legislation into an unambiguous mathematically formulated language such that proof-checkers may show that the developed code indeed satisfies the legislation. This paradigm allows us to honestly speak of error-free software.[2]

The multi-disciplinary nature of the project poses many challenges. For one, legislation is often intended to leave room for various interpretations and applications of the law. In contrast, mathematical definitions and algorithms are deterministic in nature and disallow ambiguity. The main mitigation of this challenge seems to be the accepted tendency to require unambiguous laws if they should prescribe an algorithm. These laws are written in prose, and albeit technical, it will always leave room for multiple interpretations which sometimes only differ on very subtle yet essential aspects. Here jurisdiction tells us what to do in most cases. Our collaboration with working lawyers has been very interesting in this aspect.

Yet another challenge lies in choosing the right ontology and logico-mathematical framework where to recast the interpreted and disambiguated laws. It is mainly this aspect that is addressed here. In particular, in this paper we will argue that the European regulation can be modelled in linear temporal logics [10], broadly construed as subsystems and extensions of the classical LTL with "until".

To illustrate this claim we identify some passages that may be problematic from a logical perspective, most notably because they contain *prima facie* "impredicative" content: for our purposes, a property is *impredicative* if its definition requires genuine quantification over the set of all subsets of $\mathbb{N}$. This terminology is inspired from Weyl's predicative mathematics which does not accept the powerset axiom for infinite sets [11]. Nevertheless, all laws we consider will fall in the Σ^1_1 fragment of monadic second-order logic, and model-checking formulas in this fragment can be reduced to satisfiability of first-order formulas. Thus we argue that such laws are not ideal from a computational perspective, but even in the worst case scenario, checking the compliance of a law can be reduced to a well-understood problem.

2 European Transport Law

In this section we discuss some passages from the European transport regulation [3] and why they pose a challenge in terms of logical modelling. Our analysis will be based on the following excerpts, which we have found to be problematic from a logical perspective.

[2] Of course, it has its subtleties. Software will be as good as the specification, which may contain errors. Also, we must trust the small kernel of the proof-checker, apart from the hardware and middleware involved. There is also the consistency assumption of the underlying type-theory. A further methodological objection may be that the formalisations and proofs are not easily human-readable.

§4(h) "regular weekly rest period" means any period of rest of at least 45 hours.

§4(i) "a week" means the period of time between 00.00 on a Monday and 24.00 on the following Sunday.

§8.6. In any two consecutive weeks, a driver shall take at least:

- two regular weekly rest periods, or
- one regular weekly rest period and one reduced weekly rest period of at least 24 hours. However, the reduction shall be compensated by an equivalent period of rest taken en bloc before the end of the third week following the week in question.

A weekly rest period shall start no later than at the end of six 24-hour periods from the end of the previous weekly rest period.

§8.7. Any rest taken as compensation for a reduced weekly rest period shall be attached to another rest period of at least nine hours.

§8.9. A weekly rest period that falls in two weeks may be counted in either week, but not in both.

▶ Remark 1. There are additional regulations regarding *daily* rest periods. For the sake of exposition we will only consider the above-mentioned regulations, but in all constructions and examples it should be noted that the driver would additionally have to rest daily in order to fully comply with the law. We will not discuss daily resting periods further in this text.

2.1 Placement of weekly rest periods

Let us consider a case implied by Article §8 of the Regulation, depicted in Figure 1. Each letter-divided segment denotes a week and the smaller segments denote a day, with time flowing from left to right. Furthermore, each serpentine line denotes weekly rest periods of 68 hours except the last one, which lasts only 45 hours.

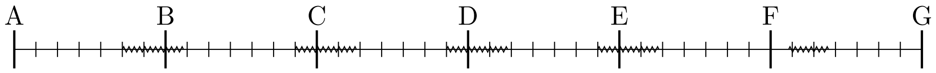

Figure 1 Six consecutive *weeks* and five weekly rest periods (serpentine lines) taken by a hypothetical driver.

Figure 1 represents the activities of a driver who starts resting Saturday at 00:00h and retakes their activity on Monday at 20:00h. Then, until the fourth week, the driver periodically start his weekly rest on Sunday at 00:00h and retake their activity on Tuesday at 20:00h. During the sixth week they rest 45 hours, from Monday at 20:00h to Wednesday at 17:00h.

Since all except the last of these weekly rest periods fall between two weeks, it is reasonable to want to find a procedure that will determine whether there exists a way of counting each of them within one week or the other as per §8.9, so that the situation becomes legal.

In our simple example, the segment FG has a fixed rest period of 45 hours. In the remaining weeks we have to choose where to assign the resting periods,[3] but it is evident that we cannot arrange them in a way that makes the whole interval AG legal. One might argue that this situation is a bit controversial, given that all other articles exposed above except §8.9 are complied beyond their minimum requirements.

[3] We cannot assign parts of this periods to different weeks, since this would give rise to two consecutive reduced weekly rest periods and thus violate §8.6.

Here, the Regulation does not pose a logical problem, nor is it inconsistently worded. But logic is not entirely unrelated to this issue. The complexity that results from §8.9 generates a potential combinatorics problem. As an example, we could encounter situations which follow the structure from Figure 1 with many more occurrences of the *in between* segments. Verifying the legality of the situation could, in principle, require checking a large number of possible assignments of rest intervals to weeks. This non-locality feature has been discussed and formalised in Coq [2].

In a first attempt to formally represent §8.9 we may think in a second-order setting: we could model weekly rest periods as pairs of points indicating the start and end of the rest. Thus §8.9 could be a formula asserting the existence of a function that would model the assignment of weekly rest periods into weeks. Such a formalization would require a second-order existential quantifier (and, in fact, would even fall outside of monadic second order logic, which does not allow for function quantification). In the following section we discuss this issue in some detail.

2.2 Timing of compensations

The second potential source of problems comes from the compensation mechanism of §8.6. To illustrate it, we construct weeks A, B, and $C_i, 1 \leq i \leq n$ such that the sequences $[A, C_1, \ldots, C_n]$ and $[C_1, \ldots, C_n, B]$ are both legal, but the full sequence $[A, C_1, \ldots, C_n, B]$ is *not.* The question then arises: *where is the illegality?* It is in the combination between A and B, where A and B can be arbitrarily far apart from each other. Clearly this is not a good feature for a law.

Throughout this subsection, line segments represent weeks, and the numbers attached to them represent the number of hours rested during each week. In Figure 2, the first and last segments represent the weeks A and B we mentioned before.

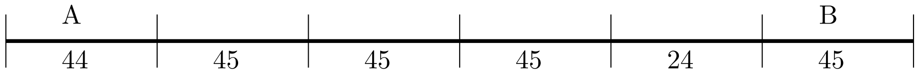

Figure 2 Illegal interval of six consecutive weeks performed by a hypothetical driver.

As shown in Figure 3, if we do not consider the last week, the remaining interval is rendered legal by the law, for we can assume that the hours to be compensated will be incorporated in the week we omitted.

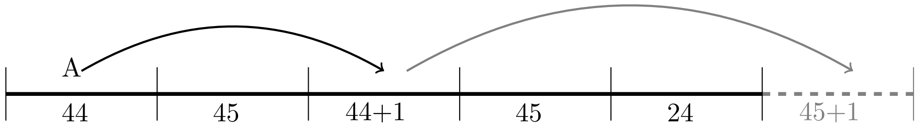

Figure 3 First five weeks of the example represented in Figure 2, together with a possible sixth week that would make the whole interval legal.

Similarly, if we remove week A from the example of Figure 2, the resulting interval (represented in Figure 4) is also legal, since we can assume that the compensation for the fourth week takes place in the weeks outside our interval.

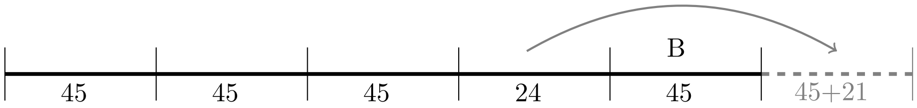

Figure 4 Last five weeks of the interval represented in Figure 2, together with a possible sixth week that would make the whole interval legal.

However, the interval of Figure 2 is illegal, as Figure 5 illustrates. This is because after compensating the first week according to article §8.6, we still have to compensate one hour, but we cannot allocate it within any of the three following weeks without having two consecutive reduced weekly rest periods.

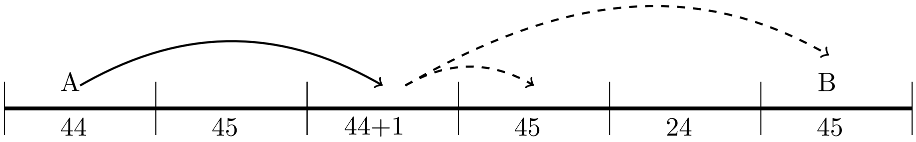

Figure 5 The same interval of Figure 2, with an attempt to assign compensations (dashed lines) that ultimately fails.

This example can be generalized to ensure that that A and B are n weeks apart. The corresponding interval (illustrated in Figure 6) has a similar structure to the one we have treated. The first week has a 44 hour weekly rest period, and all the following weeks have 45 hour weekly rest periods except for the penultimate one, which has a 24 hour weekly rest period.

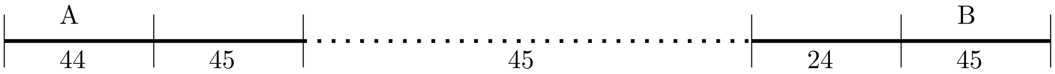

Figure 6 General example of an illegal interval that is legal when week A or week B is erased.

In this situation if we omit one of the weeks A or B the remaining interval will be legal, but the interval as it stands is illegal.

Indeed, a literal reading of the law would require three functions c_1, c_2, c_3 where given a week W, $c_i(W)$ is a (possibly empty) interval that occurs i weeks later and is used to compensate a reduced weekly rest. Once again such functions are not, properly speaking, objects of monadic second order logic, but we will show that they can be represented as such.

In the rest of the article we will show that these properties can indeed be represented in monadic second order logic, and explore whether simpler representations are possible. Before we do so, let us review the logical frameworks we will work with.

3 Temporal Logics

In this section we review the temporal logics that we consider. These are all subsystems of either linear temporal logic LTL or monadic second-order logic MSO interpreted over the natural numbers; as we discuss below, we regard the latter as a temporal logic in view of Kamp's theorem and extensions.

3.1 Linear Temporal Logic

Linear temporal logic is based on the language $\mathcal{L}_{\Box\,\mathsf{U}}$ given by the following grammar:

$$\varphi, \psi \ := \ \bot \mid P \mid \varphi \to \psi \mid \bigcirc\varphi \mid \Box\varphi \mid \varphi\,\mathsf{U}\,\psi,$$

where P is an element of a countable set $\mathbb{P}$ of predicate symbols. We will consider the U-free fragment $\mathcal{L}_{\Box}$, the $\Box$-free fragment $\mathcal{L}_{\mathsf{U}}$ and the language whose only tense is $\bigcirc$, $\mathcal{L}_{\bigcirc}$. As usual, $\bigcirc$ is read as "next", $\Box$ is read as "henceforth", and U as "until". We define other Booleans and $\Diamond$ as abbreviations in the standard way. Note that $\mathcal{L}_{\mathsf{U}}$ is expressively equivalent to $\mathcal{L}_{\Box\,\mathsf{U}}$, so we will seldom work over the full language. We could additionally consider past tenses, but they do not add expressive power to $\mathcal{L}_{\mathsf{U}}$ in models with a starting point (although there are issues with succinctness which we briefly discuss).

The articles we consider also require some counting, but this can be dealt with using the following abbreviations, where $n, m \in \mathbb{N}$. Below, an empty disjunction should be read as $\bot$ and an empty conjunction as $\top$.

- $\bigcirc^0\varphi := \varphi$ and $\bigcirc^{n+1}\varphi = \bigcirc\bigcirc^n\varphi$;
- $\Diamond^{<n}\varphi = \bigvee_{i=0}^{n-1}\bigcirc^n\varphi$ and $\Box^{<n}\varphi = \bigwedge_{i=0}^{n-1}\bigcirc^n\varphi$.

Variants with $\leq n$ instead of $<n$ are defined by reading $\leq n$ as $<n+1$.

Given any formula φ and a set $\Theta \subseteq \{\bigcirc, \Box, \mathsf{U}\}$, we define the Θ-*depth* of φ (in symbols, $\mathrm{dpt}_\Theta(\varphi)$) to be the nesting depth of tenses in Θ, defined in a standard way. If $\Theta = \{\vartheta\}$ we write ϑ-*depth* and $\mathrm{dpt}_\vartheta(\cdot)$ instead of Θ-depth and $\mathrm{dpt}_\Theta(\cdot)$, and if $\Theta = \{\bigcirc, \Box, \mathsf{U}\}$ we write *temporal depth* and $\mathrm{dpt}(\cdot)$ instead of Θ-*depth* and $\mathrm{dpt}_\Theta(\cdot)$. As a general rule we consider the $\bigcirc$-depth to be a negligible complexity measure with respect to the depths of other tenses.

We will always interpret formulas of $\mathcal{L}$ over the structure $(\mathbb{N}, S)$, where $S(n) = n + 1$. Hence, for our purposes an LTL *model* $\mathcal{M}$ is merely a function $\cdot^{\mathcal{M}} : \mathbb{P} \to 2^{\mathbb{N}}$. We define the satisfaction relation $\models$ inductively by

1. $(\mathcal{M}, n) \models P$ iff $n \in P^{\mathcal{M}}$
2. $(\mathcal{M}, n) \not\models \bot$
3. $(\mathcal{M}, n) \models \varphi \to \psi$ iff $(\mathcal{M}, n) \not\models \varphi$ or $(\mathcal{M}, n) \models \psi$
4. $(\mathcal{M}, n) \models \bigcirc\varphi$ iff $\big(\mathcal{M}, S(n)\big) \models \varphi$
5. $(\mathcal{M}, n) \models \Box\varphi$ iff for all $k \geq 0$ we have that $\big(\mathcal{M}, S^k(n)\big) \models \varphi$
6. $(\mathcal{M}, n) \models \varphi\,\mathsf{U}\,\psi$ iff there exists $k \geq 0$ such that $\big(\mathcal{M}, S^k(n)\big) \models \psi$ and $\forall i \in [0, k)$, $\big(\mathcal{M}, S^i(n)\big) \models \varphi$

As usual, a formula φ is *satisfiable* over a set of models Ω if there is $\mathcal{M} \in \Omega$ and $n \in \mathbb{N}$ so that $(\mathcal{M}, n) \models \varphi$, and *valid* on Ω if, for every $\mathcal{M} \in \Omega$ and $n \in \mathbb{N}$, $(\mathcal{M}, n) \models \varphi$.

3.2 Monadic Second-Order Logic

The syntax of monadic second-order logic is defined as follows. First, define a *term* to be given by the grammar

$$t \ := \ 0 \mid x \mid S(t),$$

where x belongs to some fixed set of first-order variables $\mathbb{V}$. Then, the language $\mathcal{L}^2_\forall$ is defined by the grammar

$$\varphi, \psi \ := \ \bot \mid P(t) \mid t < s \mid \varphi \to \psi \mid \forall x\, \varphi \mid \forall P\, \varphi$$

where x is a variable, t and s terms, and $P \in \mathbb{P}$. Once again we define other Booleans and $\exists$ as standard abbreviations, and define $\mathcal{L}^1_\forall$ to be the sub-language of $\mathcal{L}^2_\forall$ that does not allow quantifiers over elements of $\mathbb{P}$.

The language $\mathcal{L}^2_\forall$ is interpreted over models $\cdot^\mathcal{M} \colon \mathbb{V} \cup \mathbb{P} \to \mathbb{N} \cup 2^\mathbb{N}$ such that $x^\mathcal{M} \in \mathbb{N}$ if x is a variable and $P^\mathcal{M} \subseteq \mathbb{N}$ if P is a predicate symbol. For a variable x and $n \in \mathbb{N}$ let $\mathcal{M}[x/n]$ be the model that is the same as $\mathcal{M}$ except that $x^{\mathcal{M}[x/n]} = n$, and for $P \in \mathbb{P}$ and $A \subseteq \mathbb{N}$ define $\mathcal{M}[P/A]$ analogously. Extend $\cdot^\mathcal{M}$ to terms by defining recursively $0^\mathcal{M} = 0$ and $(S(t))^\mathcal{M} = t^\mathcal{M} + 1$. The satisfaction relation is then defined as follows:

1. $\mathcal{M} \not\models \bot$
2. $\mathcal{M} \models P(t)$ iff $t^\mathcal{M} \in P^\mathcal{M}$
3. $\mathcal{M} \models \varphi \to \psi$ iff $\mathcal{M} \not\models \varphi$ or $\mathcal{M} \models \psi$
4. $\mathcal{M} \models \forall x\, \varphi$ iff for all $n \in \mathbb{N}$, $\mathcal{M}[x/n] \models \varphi$
5. $\mathcal{M} \models \forall P\, \varphi$ iff for all $A \subseteq \mathbb{N}$, $\mathcal{M}[P/A] \models \varphi$

Satisfiability and *validity* are defined as before. MSO denotes the language $\mathcal{L}^2_\forall$ endowed with these semantics, and MFO denotes MSO restricted to $\mathcal{L}^1_\forall$. In order to unify our semantics for temporal logics and MSO, we regard an LTL model $\mathcal{M}$ as an MSO model by setting $x^\mathcal{M} = 0$ for all variables, and similarly regard an MSO model as an LTL model by restricting the domain to $\mathbb{P}$.

We say that a set Ω of models is *definable* in a language $\mathcal{L} \subseteq \mathcal{L}_{\Box\mathsf{U}}$ if there is φ in $\mathcal{L}$ such that for any model $\mathcal{M}$ we have $(\mathcal{M}, 0) \models \varphi$ if and only if $\mathcal{M} \in \Omega$. Similarly, Ω is definable in $\mathcal{L} \subseteq \mathcal{L}^2_\forall$ if there is φ in $\mathcal{L}$ such that for any model $\mathcal{M}$, $\mathcal{M} \models \varphi$ if and only if $\mathcal{M} \in \Omega$. With this in mind, we may regard MFO as a temporal logic in terms of the following.

▶ **Theorem 2** (Kamp [8]). *Let Ω be a set of* LTL *models. Then, Ω is definable in $\mathcal{L}_\mathsf{U}$ if and only if it is definable in $\mathcal{L}^1_\forall$.*

There are also known extensions of LTL which are expressively equivalent to full MSO [6], but for our purposes the presentation as MSO is more convenient than such extensions. On the other hand, we will go back and forth between LTL and MFO depending on which is more convenient for the application at hand.

4 Expressibility

In this section we show how the legal articles we have considered could be represented within monadic second order logic. It is crucial to stress that the articles allow for some interpretation and thus certain elements may admit readings different from those we propose. We will also make a few simplifying assumptions for the sake of exposition. From discussions with legal experts we believe that our interpretations are reasonable modulo the aforementioned simplifying assumptions.

We assume that each natural number represents one hour, although we remark that tachograph data is processed[4] minute by minute and this would be the suitable resolution for actual implementations. Each moment in time (each hour in our presentation) is labelled by an activity of the driver: these activities are *driving, resting, availability, other work* and *unknown.*[5]

[4] Actually, tachograph data is recorded second by second and legally interpreted minute by minute. The law prescribes how minutes should be labelled depending on the tachograph data. We refer the reader to [4] for details and for various mathematical problems with this labelling.

[5] The value of *unknown* is not prescribed by the law, but it is implemented in various systems for obvious reasons.

Since the articles we analyse in this paper only involve rest periods, we consider a predicate symbol `Rest`. We also introduce a predicate symbol `Week` which holds on the first hour of each Monday. This condition can be treated model-theoretically – i.e. models are assumed to be equipped with a correct valuation for `Week` – or syntactically by the $\mathcal{L}_\Box$ axiom

$$\texttt{Week} \wedge \Box\big(\texttt{Week} \rightarrow (\bigcirc\Box^{<167}\neg\texttt{Week} \wedge \bigcirc^{168}\texttt{Week})\big)$$

(assuming that the model begins on the first hour of a Monday). LTL models satisfying this formula at zero are called *weekly models.* With this in mind, we proceed to illustrate how the legislation could be formalized. However, since we want to isolate possible sources of impredicativity, we will work with simplified variants of the legislation that are more suitable for expository purposes.

4.1 Article §8.9

Article §8.6 requires that each two week period be assigned two rest periods with some additional constraints, and §8.9 indicates how rest periods should be assigned to specific weeks. Our goal in this subsection is to explore the possible impredicativity arising from the assignment itself, independently of the additional conditions of §8.6. Every week should contain at least one 24 hour rest period, but this by itself would not be sufficient to comply with §8.6. On the other hand, a driver resting 45 hours each week would comply with §8.6, so this would be a sufficient, but not necessary, condition for compliance. In order to not commit to either condition, we will consider the following general property: when is it that each week can be assigned a rest period of at least d hours, so that each rest period intersects the week it is assigned to? This simplified condition is already *prima facie* impredicative, as it requires a function mapping rest intervals to weeks. Thus it may be surprising that it can actually be defined in first order logic (and hence in LTL).

▶ **Theorem 3.** *Given $d \in [2, 85]$ there is an $\mathcal{L}^1_\forall$-formula $\varphi = \varphi_d \in \mathcal{L}^1_\forall$ such that given any* LTL *model $\mathcal{M}$, $\mathcal{M} \models \varphi$ if and only if there is an assignment of weekly rest periods such that every week is assigned a rest period of length at least d.*

Proof. In this proof we will assume that variables range over weeks. It is clear that using our fundamental ontology this can be established in first order logic, as a week can be identified with its starting point, which is already marked by the predicate `Week`. Let $E(x)$ be a formula which holds if and only if x is a week with an *early* rest period (of length at least d) which means that it overlaps with the previous week, $L(x)$ a formula that holds if x contains a *late* rest period overlapping with the following week, and $I(x)$ be a formula that holds if and only if x is a week with an *internal* rest period disjoint from (but possibly contiguous with) any early or late rest periods in the week x.

Clearly E, I, L are first-order definable (although their definition depends on d). The condition $d \leq 85$ ensures that if $E(x) \wedge L(x)$ holds then the week x contains disjoint early and late rest periods.[6] Define $\check{E}(x) = E(x) \wedge \neg I(x) \wedge \neg L(x)$, and define $\check{I}(x)$, $\check{L}(x)$ analogously.

Then set

$$\varphi = \forall x \left(E(x) \vee I(x) \vee L(x)\right) \;\wedge\; \forall x\, \forall y \left(x < y \wedge \check{L}(x) \wedge \check{E}(y) \rightarrow \exists z \in (x, y)\; I(z)\right).$$

[6] If $E(x)$ then there are at most $d - 1 = 84$ hours in x and likewise for $L(x)$. In a week there are $7 \times 24 = 84 \times 2$ hours.

We claim that φ holds if and only if there is an assignment such that each week is assigned one rest period of length at least d. First assume that such an assignment exists. Clearly $\forall x\,\big(E(x) \vee I(x) \vee L(x)\big)$ holds, since if x were a counterexample no rest period could be assigned to the week of x.

Now, suppose that $x < y$ are such that $\check{L}(x) \wedge \check{E}(y)$, and choose x, y such that $y - x$ is minimal. Note that x is assigned to its late rest period (as this is the only one available) and y is assigned to its early rest period. It follows that there is a least $z \in (x, y]$ that is not assigned to its late rest period. By minimality $z - 1$ is assigned to its late rest period, hence z cannot be assigned to its early rest period. However, z must be assigned to *some* rest period by assumption, and since this rest period is neither early nor late, the week of z must contain some internal rest period, and $I(z)$ holds.

Now assume that φ holds and define an assignment recursively as follows. Let R be a rest period and suppose that all earlier rest periods have been assigned to some week. If R is internal, assign it to its current week. If R is late for week w and w has not been assigned a rest period, assign R to w. Otherwise, assign R to $w + 1$.

We prove by induction that every week is assigned to some rest period. Fix y and assume that all earlier weeks have been assigned to some period. We may assume that $E(y) \vee I(y) \vee L(y)$ holds, as otherwise φ automatically fails.

If $I(y)$ holds then the week of y has a rest period assigned to it. If $L(y)$ holds then the late rest period of y is assigned to it, unless an earlier one was already assigned to it. So we are left with the hypothetical case where $\check{E}(y)$ holds, and the early rest period of y has been assigned to $y - 1$. Let $x < y$ be minimal with the property that every $z \in [x, y)$ has had its late rest period assigned to it. First note that $E(x)$ fails, since otherwise $x > 0$ and either $x - 1$ has had its late rest period assigned to it, contradicting the minimality of x, or else the early rest period of x would have been assigned to the week of x by our recursion. Note also that $I(z)$ fails for all $z \in [x, y)$, since any internal rest period is automatically assigned to the current week. We conclude that $\check{L}(x)$ holds and $I(z)$ fails for all $z \in (x, y)$, thus φ fails. ◀

4.2 Article §8.6

Now that we have seen that the possibility of assigning rest periods is not itself impredicative, we isolate the compensation mechanism from the rest assignments and analyse it in a similar fashion. In order to do this, we work with *simple* models defined as the set of models $\mathcal{M}$ satisfying the following conditions.

- $\mathcal{M}$ is a weekly model.
- $(\mathcal{M}, 0) \models \Diamond\Box\texttt{Rest} \wedge \Box(\texttt{Week} \wedge \texttt{Rest} \rightarrow \Box\texttt{Rest})$.
- Given a week W, $W \cap \texttt{Rest}^{\mathcal{M}}$ is an interval.
- There are never more than 6×24 hours between two consecutive rest periods.

The idea is that all rest periods are internal (the first hour of a week is never spent resting), and so every week can unambiguously be assigned a rest period, until the driver "retires" and rests on all subsequent moments. We impose this condition to clarify that our constructions do not require "immortal" drivers. As stated previously, additional daily rest periods are needed to fully comply with regulations, but these will be ignored for the sake of exposition.

We claim that Article §8.6 admits a formalization in $\mathcal{L}^2_{\forall}$ by a Σ^1_1 formula over the class of simple models. Let R be a variable meant to denote the union of all continuous rest periods of more than nine hours and C_1, C_2, and C_3 be variables meant to denote periods of compensation: C_1 compensates the previous weekly rest, C_2 compensates the weekly rest of two weeks ago, and C_3 compensates the weekly rest of 3 weeks ago. If W is a week, let $S(W)$ be the successor week to W. We express §8.6 by a formula $\psi_{\S 8.6} := \exists R\, \exists C_1\, \exists C_2\, \exists C_3\, \psi^0_{\S 8.6}$, where $\psi^0_{\S 8.6}$ expresses a conjunction of the following conditions:

- $C_i \cap C_j = \varnothing$ if $1 \le i < j \le 3$.
- $\bigcup_{i=1}^{3} C_i \subseteq R$.
- Given a week W, $R \cap W$ is an interval of length at least 24.
- Given a week W and $i \in \{1,2,3\}$, $C_i \cap W$ is an interval. Moreover, if $C_i \cap S^i(W) \neq \varnothing$, then $C_j \cap S^j(W) = \varnothing$ for all $j \in \{1,2,3\} \setminus \{i\}$.
- Given a week W,

$$\left| \left((R \setminus \bigcup_{i=1}^{3} C_i) \cap W \right) \cup \bigcup_{i=1}^{3} (C_i \cap S^i(W)) \right| \ge 45.$$

It should be clear that each of these conditions is first order definable, hence $\psi_{\S 8.6}$ is Σ^1_1. Moreover, some inspection shows that over the set of simple models, $\psi_{\S 8.6}$ coincides with §8.6. We conclude that §8.6 admits a Σ^1_1 formalization over the set of simple models, as claimed.

▶ Remark 4. It is also possible to formalize §8.6 over the class of all weekly models using a similar Σ^1_1 formula. We restrict our attention to simple models only because the general formalization would be more cumbersome and no more illuminating.

5 Stratified Bisimulations

In this section we present a version of stratified bisimulations for $\mathcal{L}_{\mathsf{U}}$ proposed by Kurtonina and de Rijke [9]. Since all languages we consider contain Booleans and $\bigcirc$, it is convenient to begin with a “basic” notion of bisimulation for this language.

▶ **Definition 5.** *Given $k \ge 0$ and two LTL models $\mathcal{M}$ and $\mathcal{N}$, a binary relation $Z \subseteq \mathbb{N}^2$ is a k-$\bigcirc$-*bisimulation *(*between $\mathcal{M}$ and $\mathcal{N}$*) if whenever $x\ Z\ y$, $P \in \mathbb{P}$, and $j \le k$, we have $x + j \in P^{\mathcal{M}}$ iff $y + j \in P^{\mathcal{N}}$.*

We will use bounded $\bigcirc$-bisimulations as a basis to define bounded bisimulations for more powerful languages.

▶ **Definition 6.** *Fix $k \ge 0$ and two LTL models $\mathcal{M}$ and $\mathcal{N}$. Let $\vec{Z} = (Z_i)_{i=0}^{\infty}$ be a sequence such that for all $i \in \mathbb{N}$, Z_i is a k-$\bigcirc$-bisimulation and $Z_{i+1} \subseteq Z_i$.*

1. *$\vec{Z}$ is a k-$\Box$-*bisimulation (between $\mathcal{M}$ and $\mathcal{N}$) *if whenever $x\ Z_{i+1}\ y$:*
   Forth $\Box$. *For all $x' \ge x$ there exists $y' \ge y$ such that $x'\ Z_i\ y'$.*
   Back $\Box$. *For all $y' \ge y$ there exists $x' \ge x$ such that $x'\ Z_i\ y'$.*
2. *$\vec{Z}$ is a k-U-*bisimulation (between $\mathcal{M}$ and $\mathcal{N}$) *if whenever $x\ Z_{i+1}\ y$:*
   Forth U. *For all $x' \ge x$ there exists $y' \ge y$ and a function $\xi\colon [y, y'] \to [x, x']$ such that every $z \in [y, y']$ satisfies $\xi(z)\ Z_i\ z$ and $\xi(z) = x'$ if and only if $z = y'$.*
   Back U. *For all $y' \ge y$ there exists $x' \ge x$ and a function $\eta\colon [x, x'] \to [y, y']$ such that every $z \in [x, x']$ satisfies $z\ Z_i\ \eta(z)$ and $\eta(z) = y'$ if and only if $z = x'$.*

Stratified bisimulations are an essential tool in proving inexpressivity or succinctness results, given that they preserve the truth of formulas of small enough nesting depth.

▶ **Lemma 7** ([9]).

1. *Given two LTL models $\mathcal{M}$ and $\mathcal{N}$ and a k-$\Box$-bisimulation $\vec{Z}$ between them, for all formulas $\varphi \in \mathcal{L}_{\Box}$ and for all $(x, y) \in Z_i$, if φ has $\bigcirc$-depth at most k and $\Box$-depth at most i then $(\mathcal{M}, x) \models \varphi$ iff $(\mathcal{N}, y) \models \varphi$.*
2. *Given two LTL models $\mathcal{M}$ and $\mathcal{N}$ and a k-U-bisimulation $\vec{Z}$ between them, for all formulas $\varphi \in \mathcal{L}_{\mathsf{U}}$ and for all $(x, y) \in Z_i$, if φ has $\bigcirc$-depth at most k and U-depth at most i then $(\mathcal{M}, x) \models \varphi$ iff $(\mathcal{N}, y) \models \varphi$.*

In the next section we use Lemma 7 to show that certain legal properties we have considered are hard or impossible to define in fragments of linear temporal logic.

6 Non-expressibility

We have seen that Articles §8.9 and §8.6 are expressible in MFO and MSO, respectively. We will see that they are not expressible in $\mathcal{L}_\Box$ and that §8.6 is not reasonably expressible in $\mathcal{L}_\mathsf{U}$, in the sense that any formula expressing it (if it exists) would require very large U-depth. For this, we use constructions similar to the examples given in Section 2. However, since these constructions will be somewhat more elaborate, we settle some notation first.

Say that a model $\mathcal{M}$ is *eventually resting* if there is some m such that for all $n > m$ and all $P \in \mathbb{P}$, $n \in P^{\mathcal{M}}$ iff $P = \texttt{Rest}$. The *end* of an eventually resting model is the least such value of m which is also a multiple of 168 (i.e., a whole number of weeks). A week-long model is an eventually resting models whose end is 168. We define the *concatenation* of two eventually resting models $\mathcal{A}, \mathcal{B}$, denoted $\mathcal{A} \mid \mathcal{B}$, as follows. Let m be the end of $\mathcal{A}$. Then, for a predicate symbol P and $n \in \mathbb{N}$, we set

$$n \in P^{\mathcal{A}|\mathcal{B}} \Leftrightarrow \begin{cases} n \in P^{\mathcal{A}} & \text{if } n \leq m \\ n - m \in P^{\mathcal{B}} & \text{if } n > m. \end{cases}$$

If k is a natural number then $\mathcal{A}^k$ denotes k concatenated copies of $\mathcal{A}$. If $n \in [24, 168)$, then n denotes a week with one weekly resting period of n; we assume that these weekly periods fall in the middle of each week without overlapping with other weeks, with the details being non-essential. However, we do assume that any two instances of the week represented by n are identical.

It will be convenient to represent a given moment in time both by the number of hours t since the beginning of time, and by $168w + h$, where w is the number of weeks since the beginning of time, and $h < 168$ is the number of hours since the beginning of that week.

6.1 Article §8.9

We have seen that the possibility of assigning weekly rest periods to each week is first order definable. One may then ask if $\mathcal{L}_\Box$ suffices to define it, and the answer is negative. We prove this via the following construction.

▶ **Definition 8.** *Fix $d \in [24, 84]$. Define the following week-long models:*

- *E is a model whose first $\lfloor d/2 \rfloor$ hours are resting.*
- *I is a model whose hours $(\lfloor d/2 \rfloor + 1, \lfloor d/2 \rfloor + d)$ are resting.*
- *L is a model whose last $\lceil d/2 \rceil$ hours are resting.*
- *Concatenations of letters denote unions of resting hours, i.e., EL denotes a week with a beginning and an end rest period.*

Then, for each $n \in \mathbb{N}$, define the eventually resting models $\mathcal{A}_n = (L \mid EL^n \mid EIL \mid EL^n \mid E)^{n+1}$ and $\overline{\mathcal{A}}_n = L \mid EL^n \mid E \mid \mathcal{A}_n$.

Given $d \in [24, 84]$ and a model $\mathcal{M}$, we say that $\mathcal{M}$ *admits a weekly rest assignment* if it is possible that each week is assigned a weekly rest period of length at least d.

▶ **Lemma 9.** *The model $\mathcal{A}_n$ admits a weekly rest assignment but $\overline{\mathcal{A}}_n$ does not.*

Proof. It is easy to see that $\mathcal{A}_n$ satisfies the formula φ_d of Theorem 3 and that $\overline{\mathcal{A}}_n$ does not. ◀

▶ **Lemma 10.** *There is a bounded $168n$-$\Box$-bisimulation $\vec{Z}$ between $\mathcal{A}_n$ and $\overline{\mathcal{A}}_n$ such that* $0 \; Z_n \; 0$.

Proof sketch. Define $r := 2n+3$ and for $x = 168w+h, y = 168v+\ell \in \mathbb{N}$, let $x\ Z_i\ y$ if $h = \ell$ and one of the following holds:
A1. $x = y = 0$ and $i \leq n$,
A2. $0 < v$, $\max\{w, v-n-2\} \leq (n-i)r$ and $v \equiv w+n+2 \pmod{r}$, or
A3. $v = w+n+2$.
Then $\vec{Z}$ is a bisimulation (see Appendix A) and $0\ Z_n\ 0$. ◀

▶ **Theorem 11.** *Given $d \in [24, 84]$, there is no $\mathcal{L}_\Box$ formula φ such for every model $\mathcal{M}$, $\mathcal{M} \models \varphi$ if and only if $\mathcal{M}$ admits a weekly rest assignment.*

Proof. Suppose that $\varphi \in \mathcal{L}_\Box$ is such a formula. Let $d_\bigcirc$ and $d_\Box$ be its $\bigcirc$-depth and $\Box$-depth, respectively. Choose n such that $d_\bigcirc \leq 168n$ and $d_\Box \leq n$. Then by Lemmas 7 and 10, $(\mathcal{A}_n, 0) \models \varphi$ iff $(\overline{\mathcal{A}}_n, 0) \models \varphi$. But, according to Lemma 9, $\mathcal{A}_n$ admits a weekly rest assignment, while $\overline{A}_n$ does not. ◀

6.2 Article §8.6

Our goal now is to show that Article §8.6 is not expressible in $\mathcal{L}_\Box$, and that it needs a formula with a large U-depth to express it in $\mathcal{L}_\mathsf{U}$. As before, we start by defining a model that complies with the article, and one that doesn't, and then prove that they are bisimilar.

▶ **Definition 12.** *For each $n \in \mathbb{N}$, define simple models*

$$\mathcal{B}_n = (44 \mid 45^n \mid 46 \mid 45^n)^n \mid 24 \mid 45 \mid 24$$

and $\overline{\mathcal{B}}_n = 44 \mid 45^n \mid \mathcal{B}_n$.

▶ **Lemma 13.** *Given $n \in \mathbb{N}$, $\mathcal{B}_n \models \psi_{\S 8.6}$ but $\overline{\mathcal{B}}_n \not\models \psi_{\S 8.6}$.*

Proof. In $\mathcal{B}_n$, the first week's missing hour can be compensated on the third week. This creates a chain reaction of compensations, as the third week also needs to be compensated (because it's interpreted as a reduced rest of 44 hours together with a compensation of 1 hour). However, it is always possible to compensate either two weeks after, or on the week of 46 hours, if it is close enough. It is thus never necessary to use up hours from the second block of n 45 hour rest weeks, which are all regular rest periods. This process happens n times, until we reach the last three weeks of the model. Two of them need to be compensated, but it is possible to do so using the unlimited hours of rest available after the end.

Consider now $\overline{\mathcal{B}}_n$. The 24 hour weeks near the end of the model cannot be used to compensate previous weeks, since 24 is the minimum allowed weekly rest. The last 45 hour week cannot be used to compensate previous weeks either, because then there would be more than one consecutive week with no regular rest period. Thus, we erase the last three weeks from consideration. There are $m := 2n^2 + 3n + 1$ weeks in the rest of the model, $2n^2 + n$ of which have 45 rest hours, $n+1$ of which have 44 rest hours, and n of which have 46 hours, for a total of $45m - 1$ rest hours. Thus there are not enough rest hours to distribute among the period such that each week is assigned 45 hours of weekly rest. ◀

▶ **Lemma 14.** *There is a bounded $168n$-$\Box$-bisimulation $\vec{Z}$ between $\mathcal{B}_n$ and $\overline{\mathcal{B}}_n$ such that* $0\ Z_n\ 0$.

Proof. The stratified bisimulation and the proof are analogous to those used in the proof of Lemma 10. ◀

▶ **Theorem 15.** *There is no $\mathcal{L}_\Box$-formula equivalent to $\psi_{\S 8.6}$ over the class of simple models.*

Proof. Suppose that $\psi \in \mathcal{L}_\square$ is a formula expressing Article §8.6 with $\bigcirc$-depth $d_\bigcirc$ and $\square$-depth $d_\square$. Choose n big enough to ensure that $d_\bigcirc \leq 168n$ and $d_\square \leq n$, and let $\vec{Z}$ be the bisimulation of Lemma 14. Then by Lemma 7, $(\mathcal{B}_n, 0) \models \psi$ iff $(\overline{\mathcal{B}}_n, 0) \models \psi$. This contradicts Lemma 13. ◀

Now we show that any formula of $\mathcal{L}_\mathsf{U}$ requires nesting depth 20 of U.

▶ **Definition 16.** *For $n \in \mathbb{N}$, define models $\mathcal{C}_n = (44 \mid 45^{2n+1})^{21} \mid 66 \mid 24 \mid 45 \mid 24$ and $\overline{\mathcal{C}}_n = (44 \mid 45^{2n+1}) \mid \mathcal{C}_n$.*

▶ **Lemma 17.** *Given $n \in \mathbb{N}$, $\mathcal{C}_n \models \psi_{§8.6}$ but $\overline{\mathcal{C}}_n \not\models \psi_{§8.6}$.*

Proof. First we see that $\mathcal{C}_n \models \psi_{§8.6}$. Intuitively, even weeks are compensated two weeks later, and the size of the compensation increases by one every $2n+2$ weeks. Thus for example one hour of week 0 is compensated by one hour of week 2, which is compensated by one hour of week 4, and so on until we reach week $2n+2$. Note however that this week only has 44 hours of rest and has used one hour to compensate the previous week, so we need to compensate two hours of rest. This is compensated by two hours on week $2n+4$, and so on until we reach the third 44 hour rest. Since two hours of this rest are used to compensate a previous week, now three hours need to be compensated, and so on. On week $21(2n+2)$ we use 21 hours to compensate, which is the maximum allowed given that each week requires a 24 hour rest period. As before, the last $24 \mid 45 \mid 24$ block cannot be used to compensate, but can be compensated with the following unlimited rest.

More formally, every week w numbered $2k$ (including week zero) will be reduced and compensated by week $2k+2$, up to and including week $21(2n+2)$. The amount of the compensation is the unique $i > 0$ such that $(i-1)(2n+2) \leq w < i(2n+2)$.

As in $\overline{\mathcal{B}_n}$, the $24 \mid 45 \mid 24$ block at the end of $\overline{C}_n$ cannot be used to compensate previous weeks (see the proof of Lemma 13). There are $m := 22(2n+2)+1$ remaining weeks in $\overline{C}_n$, of which $22(2n+1)$ have 45 resting hours, 22 have 44 resting hours, and 1 has 66 resting hours, for a total of $45m - 1$ resting hours. Thus there are not enough resting hours to distribute among the weeks. ◀

▶ **Lemma 18.** *There is a bounded $168n$-U-bisimulation $\vec{Z}$ between $\mathcal{C}_n$ and $\overline{\mathcal{C}}_n$ such that $0 \; Z_{20} \; 0$.*

Proof sketch. Let $r := 2n+2$. For $168w+h \in \mathcal{C}_n$ and $168v+\ell \in \overline{\mathcal{C}}_n$, set $168w+h \; Z_i \; 168v+\ell$ if $h = \ell$ and one of the following holds:

C1. $\max\{w+r, v\} < (21-i)r$ and $w \equiv v \pmod{r}$;

C2. $v = w + r$.

Then, $\vec{Z}$ is a stratified bisimulation (see Appendix A) and $0 \; Z_{20} \; 0$ by C1. ◀

▶ **Theorem 19.** *Any $\mathcal{L}_\mathsf{U}$ formula equivalent to $\psi_{§8.6}$ has U-depth at least 20.*

Proof. Suppose that $\psi \in \mathcal{L}_\mathsf{U}$ is a formula expressing Article §8.6 with $\bigcirc$-depth d and U-depth less than 20. Choose n big enough to ensure that $d \leq n$, and let $\vec{Z}$ be the bisimulation of Lemma 18. Then by Lemma 7, $(\mathcal{C}_n, 0) \models \psi \iff (\overline{\mathcal{C}}_n, 0) \models \psi$. This contradicts Lemma 17. ◀

▶ Remark 20. One can ask how Theorem 19 would differ if we included "since" in the language. In this case, $(\mathcal{C}_n, 0)$ and $(\overline{\mathcal{C}}_n, 0)$ are only about 10-bisimilar. However, the nesting depth of 20 is determined only by the resolution of our models. If instead we used a minute-wise resolution (which, as we have mentioned, is the resolution required by the law itself), we could stretch this to 20×60 by replacing the 44 hour reduced weekly rests by $44:59$ reduced weekly rests. Thus any LTL definition of $\psi_{\S 8.6}$ would have to exploit the temporal resolution in an essential way, making it arguably unnatural.

7 Concluding Remarks

We have shown that the Σ^1_1 fragment of monadic temporal logic is sufficient for formalizing even the most problematic passages we have found in our study of European transport regulations. The upshot is that evaluating whether a given truck driver's record complies with regulations can then be transformed into a model-checking problem over this fragment. Moreover, truth of Σ^1_1 MSO formulas is equivalent to validity for MSO, and via Kamp's theorem we may further reduce it to validity of LTL formulas, for which many algorithms and solvers are already available. Nevertheless, validity in LTL is PSPACE-complete, and moreover the translation of MSO into LTL is non-elementary in the worst case, so this approach is not ideal from a complexity perspective.

On the other hand, LTL is indeed suitable for formalizing portions of the regulation, and in this case the model-checking problem (over deterministic models) is polynomial [5]. In fact, the advantage of having such a general tool available can be viewed as an argument to use "sugared" versions of LTL (say, with counting modalities) in the design of future – and revision of current – laws.

Indeed, consider the following variant of §8.6:

- In every two consecutive weeks, the driver must take two weekly rest periods, at least one of which is regular.
- In every four consecutive weeks, the sum of the weekly rest periods must be of at least 180 hours.

This version of the article can be easily checked to be definable by a not-too-large LTL formula and maintain the spirit of the original, as drivers are required to compensate reduced rest periods within the following three weeks.

A second issue concerns the use of classical logic. This is especially relevant when the law is ambiguous or contradictory, or driving records are incomplete. Up to now our team has found classical logic to be sufficient for our intended applications, but it is possible that some non-classical temporal logic (as in e.g. [1, 7]) will turn out to be the "right" foundation for modelling these regulations.

References

1 J. Boudou, M. Diéguez, and D. Fernández-Duque. A Decidable Intuitionistic Temporal Logic. In *26th EACSL Annual Conference on Computer Science Logic (CSL)*, pages 14:1–14:17, 2017.

2 J. del Castillo Tierz. When the laws of logic meet the logic of laws. Master's thesis, University of Barcelona, Barcelona, 2018. URL: `http://diposit.ub.edu/dspace/handle/2445/133778`.

3 European Parliament and Council of the European Union. Regulation (EC) No 561/2006 of the European Parliament and of the Council of 15 March 2006 on the harmonisation of certain social legislation relating to road transport and amending council regulations (EEC) No 3821/85 and (EC) No 2135/98 and repealing council regulation (EEC) No 3820/85 (text with EEA relevance) - declaration. Official Journal of the European Union, 2006. URL: `https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006R0561`.

4 D. Fernández-Duque, M. González Bedmar, D. Sousa, J.J. Joosten, and G. Errezil Alberdi. To Drive or Not to Drive: A Formal Analysis of Requirements (51) and (52) from Regulation (EU) 2016/799. Submitted, 2019.

5 D. Harel, J. Tiuryn, and D. Kozen. *Dynamic Logic*. MIT Press, Cambridge, MA, USA, 2000.

6 J.G. Henriksen and P.S. Thiagarajan. Dynamic Linear Time Temporal Logic. *Annals of Pure and Applied Logic*, 96(1-3):187–207, 1999. doi:10.1016/S0168-0072(98)00039-6.

7 N. Kamide and H. Wansing. A Paraconsistent Linear-time Temporal Logic. *Fundamenta Informaticae*, 106(1):1–23, 2011. doi:10.3233/FI-2011-374.

8 H. Kamp. *Tense Logic and the Theory of Linear Order*. PhD thesis, UCLA, 1968.

9 N. Kurtonina and M. de Rijke. Bisimulations for Temporal Logic. *Journal of Logic, Language and Information*, 6(4):403–425, 1997.

10 O. Lichtenstein and A. Pnueli. Propositional Temporal Logics: Decidability and Completeness. *Logic Jounal of the IGPL*, 8(1):55–85, 2000.

11 H. Weyl. *The Continuum: A Critical Examination of the Foundation of Analysis*. Mineola: Dover, 1994.

A Bisimulation proofs

Recall the models $\mathcal{A}_n = (L \mid EL^n \mid EIL \mid EL^n \mid E)^{n+1}$ and $\overline{\mathcal{A}}_n = L \mid EL^n \mid E \mid \mathcal{A}_n$.

▶ **Lemma 10.** *There is a bounded* $168n$-$\Box$-*bisimulation* $\vec{Z}$ *between* $\mathcal{A}_n$ *and* $\overline{\mathcal{A}}_n$ *such that* $0\ Z_n\ 0$.

Proof. Define $r := 2n+3$ and for $x = 168w+h, y = 168v+\ell \in \mathbb{N}$, let $x\ Z_i\ y$ if $h = \ell$ and one of the following holds:

A1. $x = y = 0$ and $i \le n$,

A2. $0 < v$, $\max\{w, v-n-2\} \le (n-i)r$ and $v \equiv w+n+2 \pmod r$, or

A3. $v = w+n+2$.

We need to show that $\vec{Z}$ is a stratified bisimulation.

It is clear that $Z_{i+1} \subseteq Z_i$. Assume that $x\ Z_i\ y$ and write $x = 168w+h$, $y = 168v+\ell$; note that by definition we must have $h = \ell$. If $i = 0$, then some inspection shows that x and y share the same formulas of the form $\bigcirc^j p$ with $j \le 168n$, since the current and subsequent n weeks are of the same form. It is sufficient to check this for Z_0 because it contains all the Z_i.

Otherwise, change variables so that $x \sim_{i+1} y$; we check that the required clauses hold.

Forth $\Box$. Let $x' \ge x$ and write $x' = 168w'+h'$. We claim that there is v' such that $168v'+h' \ge 168v+h$ and $168w'+h'\ Z_i\ 168v'+h'$. If $168(w'+n+2)+h' \ge 168v+h$ we may take $v' = w'+n+2$, and the bisimulation holds by A3. Otherwise, we have $v \ge w'+n+2 \ge w+n+2$, where the first inequality is strict unless $h' < h$, in which case the second inequality must be strict. Hence x, y do not satisfy A1 nor A3 and thus $\max\{w, v-n-2\} \le (n-i-1)r$. Take $v' \in (v, v+r]$ with $v' \equiv w'+n+2 \pmod r$ and set $y' = 168v'+h'$. Note that $w'+n+2 \le v < (n-i-1)r+n+2$ yields $w' \le (n-i)r$, while $v' \le v+r \le (n-i-1)r+r = (n-i)r$, and thus $v-n-2 \le (n-i)r$ as well. Thus $x'\ Z_i\ y'$ by A2.

Back $\Box$. Let $y' \ge y$ and write $y' = 168v'+h'$. As before, we claim that there is w' such that $168w'+h' \ge 168w+h$ and $168w'+h'\ Z_i\ 168v'+h'$. If $168(v'-n-2)+h' \ge 168w+h$ we may take $w' = v'-n-2$, and the result follows by A3. Otherwise, we have $w \ge v'-n-2 \ge v-n-2$ with one inequality being strict , so that x, y do not satisfy A3. If x, y satisfy A2, then $\max\{w, v-n-2\} \le (n-i-1)r$. If x, y satisfy A1, we have that $w = v = 0$ and $i+1 \le n$, so that $\max\{w, v-n-2\} = 0 \le (n-i-1)r$ as well. Take $w' \in (w, w+r]$ with $w'+n+2 \equiv v' \pmod r$ and set $x' = 168w'+h'$. It is not hard to check that $\max\{w', v'-n-2\} \le (n-i)r$, and thus $x'\ Z_i\ y'$ by A2. ◀

Recall the models $\mathcal{C}_n = (44 \mid 45^{2n+1})^{21} \mid 66 \mid 24 \mid 45 \mid 24$ and $\overline{\mathcal{C}}_n = (44 \mid 45^{2n+1}) \mid \mathcal{C}_n$.

▶ **Lemma 18.** *There is a bounded* $168n$*-U-bisimulation* $\vec{Z}$ *between* $\mathcal{C}_n$ *and* $\overline{\mathcal{C}}_n$ *such that* $0 \; Z_{20} \; 0$.

Proof. Recall that we defined $r := 2n+2$ and for $168w + h \in \mathcal{C}_n$ and $168v + \ell \in \overline{\mathcal{C}}_n$, we set $168w + h \; Z_i \; 168v + \ell$ if $h = \ell$ and one of the following holds:

C1. $\max\{w + r, v\} < (21 - i)r$ and $w \equiv v \pmod r$, or

C2. $v = w + r$.

We need to show that $\vec{Z}$ is a stratified bisimulation. To see this, assume that $x \; Z_i \; y$ and write $x = 168w + h$, $y = 168v + \ell$. Note that we must have $h = \ell$. If $i = 0$ then some inspection shows that x and y share the same formulas of the form $\bigcirc^j p$ with $j \le 168n$, as the current and subsequent n weeks are of the same form. It is sufficient to check this for Z_0 because it contains all the Z_i.

If $i > 0$, change variables so that $x \sim_{i+1} y$; we check that the required clauses hold.

Forth U. Let $x' \ge x$ and write $x' = 168w' + h'$. Consider two cases. First assume that $w' \le w + r$. Set $y' = y + (x' - x)$ and for $z \in [y, y']$ set $\xi(z) = x + (z - y)$. It is then not hard to check that if $x \; Z_{i+1} \; y$ by C1 then $\xi(z) \; Z_i \; z$ by C1, and similarly if $x \; Z_{i+1} \; y$ by C2 then $\xi(z) \; Z_i \; z$ by C2. The other required properties of ξ are easy to check, so that ξ witnesses Forth U.

Otherwise $w' > w + r$. We claim that there is v' such that $168v' + h' \ge 168v + h$ and $168w' + h' \; Z_i \; 168v' + h'$. If $168(w' + r) + h' \ge 168v + h$ we may take $v' = w' + r$. Otherwise, we have $v \ge w' + r > w + r$ so that x, y do not satisfy C2 and thus $\max\{w + r, v\} \le (21 - i - 1)r$. Take $v' \in (v, v + r]$ with $v' \equiv w' \pmod r$ and set $y' = 168v' + h'$; from $(21 - i - 1)r \ge v \ge w' + r$ and $v' \le v + r \le (21 - i)r$ we obtain $x' \; Z_i \; y'$ by C1.

We now construct the function $\xi \colon [y, y'] \to [x, x']$. First define $\xi(y') = x'$. For $z = 168u+t \in [y, y')$, we consider two cases. If $168(u-r)+t \in \big[x, x'\big)$ take $\xi(z) = 168(u-r)+t$, which in view of C2 satisfies all desired properties. Otherwise, $168(u - r) + t \notin [x, x')$, and choose $d \in (0, r]$ such that $w + d \equiv u \pmod r$, then set $\xi(z) = 168(w + d) + t$. The assumption that $w' > w + r$ yields $\xi(z) \in [x, x']$. It remains to show that $\xi(z) \; Z_i \; z$, for which it suffices to check that $\max\{w + d + r, u\} < (21 - i)r$.

If $168(u-r)+t < x$ then since $z \ge y$, either $u > v$ and hence $v < u \le w+r$, or else $u = v$ and $t \ge h$, so that forcibly $u - r < w$ and thus $v < w + r$. But $v < w + r$ together with $168v+h' \; Z_{i+1} \; 168w+h$ means that C1 holds so that $\max\{w+r, v\} < (21-i-1)r$. Thus we have $u-r \le w < (21-i-1)r$ so that $u < (21-i)r$. Similarly $w+d \le w+r < (21-i-1)r$ yields $w + d + r < (21 - i)r$.

Otherwise $168(u - r) + t \ge x'$. But then since $z < y'$, either $u = v'$ and hence $t < h'$, so that $v' - r = u - r > w'$; or else $u < v'$ and $v' - r > u - r \ge w'$. Thus $w' + r \ne v'$, which together with $168w' + h' \; Z_i \; 168v' + h'$ yields $\max\{w' + r, v'\} < (21 - i)r$. From $u \le v' < (21 - i)r$ and $w + d + r \le (w + r) + r < w' + r < (21 - i)r$ we obtain $\max\{w + d + r, u\} < (21 - i)r$, as needed.

Back U. This is essentially symmetric and we omit it. ◀