To Drive or Not to Drive*

A Formal Analysis of Requirements (51) and (52) from Regulation (EU) 2016/799

David Fernández Duque[1], Mireia González Bedmar[2], Daniel Sousa[3], Joost J. Joosten[4], and Guillermo Errezil Alberdi[5]

[1,2,3,4] *Department of Philosophy, Universitat de Barcelona*
[5] *Formal Vindications S.L. and Guretruck S.L.*

Abstract: When a regulation lays down the specifications of automatic procedures to be implemented as software, several features should be met: unambiguous prose, computational feasibility and, we believe, avoidance of chaotic behaviour. This article analyses Requirements (51) and (52) from Regulation (EU) 2016/799 with the goal of identifying several glitches, from ambiguity in the intended order of application to diametrically opposite results depending on small and, we believe, meaningless, variations of the input. Directed to an interdisciplinary audience, this document provides mathematical proofs of our claims, along with natural-language accounts of our main results.

Keywords: algorithmic law, formal analysis of laws, automated law enforcement, leap seconds, tachograph

*This paper is part of the project RTC-2017-6740-7 funded by the "Ministry of Science, Innovation and Universities", the "State Agency for Research" and the "European Regional Development Fund" (ERDF).

1 Introduction

Regulation (EU) 2016/799 lays down the requirements for the construction, testing, installation, operation and repair of tachographs —digital devices which record the activities of road transport drivers. We analyse Requirements (51) and (52) of the regulation with the goal of identifying problematic behaviour.

Tachographs are to road vehicles what black boxes are to airplanes. As such, each second they record an activity that has been performed (e.g. driving, resting). However, tachographs are required to output one activity per minute. Requirements (51) and (52) are meant to prescribe how to label minutes according to the recorded labelling of seconds.

They read as follows:

> (51) Given a calendar minute, if DRIVING is registered as the activity of both the immediately preceding and the immediately succeeding minute, the whole minute shall be regarded as DRIVING.
>
> (52) Given a calendar minute that is not regarded as DRIVING according to requirement 051, the whole minute shall be regarded to be of the same type of activity as the longest continuous activity within the minute (or the latest of the equally long activities).

We have identified two main issues. The first one has to do with the intrinsic ambiguity of the phrasing, and concerns the order in which these two requirements shall be applied. Although (52) explicitly refers to (51) and hence suggests that it must follow after (51), the reading of (51) and its context within the regulation reveals that it is negligent on its terms (since no minute activities have been registered) and has no effect when applied first. We treat these considerations in a mathematical setting in Section **??**.

The second issue arises from the use of the expression “calendar minute”. A first critique is that the term is not explicitly defined in the regulation and, even worse, is not consistent with its translations into other languages[1]. An indulgently reasonable interpretation of “calendar minute” is the period of time between a date-time of the calendar ending in $h{:}m{:}00$ and the beginning of the next minute of the calendar. The discordance arises because different time standards (or calendars) have minutes starting at different points of time, and the shift between two calendars can in fact change the outcome of applying Requirement (52) to the labelling of seconds. Section **??** proves mathematically that the same labelling of seconds can end up being assigned drastically conflicting interpretations depending on the calendar standard used.

[1] The Spanish version says *un minuto cualquiera*, “any minute”, while the Italian says *un intervallo di un minuto*, “an interval of a minute”.

Regulation (EU) 2016/799 prescribes the use of the UTC calendar, which in its definition incorporates leap seconds — extra seconds added to certain days in order to compensate the variations of the Earth's rotation speed. Due to the existence of leap seconds, the UTC calendar has a shift with respect to other usual timekeeping systems (as of April 2019, the shift is 27 seconds with respect to UT1). Thus calendar minutes start at different instants on UTC and UT1. Tachographs encode the time at which some activity has happened using a timestamp, i.e., the number of seconds elapsed since midnight of 1 January 1970. Such leap seconds should be taken into account given that the use of UTC is prescribed by the law. However, experimental tests show that tachographs perform the algorithm of minute labelling disregarding leap seconds, i.e., assuming that the timestamp does not count leap seconds. This entails a violation of the law and may lead to disastrous discrepancies on the output of computations.

Regulation (EU) 2016/799 lays down the behaviour of automatic procedures applied in law enforcement. In this area, unambiguous specifications and fully deterministic behaviour is essential; otherwise, the engineers making the hardware and writing the software are left to make the decisions — consciously or not — regarding how the law is to be interpreted.

This text is structured as follows. Section **??** exposes the changes in Regulation (EU) 2016/799 and previous regulations before their current shape. Sections **??**, **??**, and **??** are of a mathematical nature and may be skipped by readers not interested in technical details. Section **??** presents the findings of the previous sections in a language suitable to the reader not familiar with mathematical prose. Section **??** sketches the results of experiments with real-world data conducted by Guretruck S.L. Finally, Section **??** summarizes our conclusions.

2 Intended interpretation

Requirement (51) is problematic in that it refers to an activity being registered as the one of the preceding and succeeding minute, with no previous reference to when an activity is considered registered. To be able to apply Requirement (51), one needs to have previously registered some activity, and only in (52) is a criterion for doing so established.

However, since Requirement (52) references Requirement (51), it seems clear that in some sense (51) precedes (52). One possible interpretation is that the requirements are to be applied as many times as needed to satisfy both statements: we would have the chain of applications (51)-(52)-(51)-(52)-.... In Section **??** we will prove that this sequence of applications is equivalent to the sequence (52)-(51).

Another interpretation, which in a legal context might seem more customary, is that the requirements are to be applied in the order of appearance, (51)-(52). In this case, after the application of (52) it is possible to reach a configuration that violates (51), as we shall see in Section **??**.

In any case, the ambiguity of the regulation is undeniable. If we trace these requirements back in time, what we find is disheartening. Before the passing of Regulation (EU) 2016/799, Council Regulation (EEC) 3821/85 was enforced, which in its first version says:

> 040 Given a calendar minute, if any DRIVING activity has occurred within the minute, the whole minute shall be regarded as DRIVING.
>
> 041 Given a calendar minute, if any DRIVING activity has occurred within both the immediately preceding and the immediately succeeding minute, the whole minute shall be regarded as DRIVING.
>
> 042 Given a calendar minute that is not regarded as DRIVING according to previous requirements, the whole minute shall be regarded to be of the same type of activity as the longest continuous activity within the minute (or the latest of the equally longest).

The first sentence, which was removed later by an amendment in Commission Regulation (EU) 1266/2009, changes the global meaning of the excerpt. In this version, it seems clear that the two first sentences, applied in the order as they appear, determine which minutes are registered as DRIVING, and the third sentence will only be applied in order to register the other activities. However, after amendment Commission Regulation (EU) 1266/2009, Requirement 040 was removed and Requirements 041 and 042 were rephrased to match the current (51) and (52).

In this paper, we will restrict our attention to the legal text in its current form, despite it being ambiguous and insufficient to accomplish an algorithmic description of the labelling of minutes.

3 Formal definitions

In this section we will formalize the concepts and terminology we will use. The reader who is not interested in the mathematical details of our claims can skip to Section **??**.

We are given a list of consecutive seconds with their activity assigned by the tachograph. To represent the seconds, we will use the integer numbers $\mathbf{Z}$ (we extend backward and forward for simplicity, which is no problem since we can assume an UNKNOWN activity for all the seconds out of range). The space of activities will be $\mathbf{A} := \{$DRIVING, REST, AVAILABILITY, WORK, UNKNOWN}. A labelling is any function $f : \mathbf{Z} \to \mathbf{A}$. We will use the following convention: when $\mathbf{Z}$ is being interpreted as seconds, we will say that $S : \mathbf{Z} \to \mathbf{A}$ is a second labelling, and when $\mathbf{Z}$ is interpreted as minutes, we will say that $M : \mathbf{Z} \to \mathbf{A}$ is a minute labelling.

Now, to deal with time shifts, we use $\mathbf{Z}$ also to represent the list of minutes of the calendar and we encode a shift as an integer $d \in \mathbf{Z}$. The set $\mathbf{Z}_{60}$ is the set of the integers from 0 to 59, both included. We convert seconds to pairs consisting of a minute and a second of minute through a function $c^d : \mathbf{Z} \to \mathbf{Z} \times \mathbf{Z}_{60}$ which for every second $s \in \mathbf{Z}$ is defined as:

$$c^d(s) := \left(\left\lfloor \frac{s-d}{60} \right\rfloor, (s-d)\%60 \right),$$

where % denotes the remainder from the euclidian division. We use c_0^d for the first component and c_1^d for the second component of the above function c^d.

So, in summary, the calendar is such that minute 0 starts exactly at second d, minute 1 starts at second $d + 60$, and so on.

Example 3.1. Given a shift $d = 0$, we have that $c^0(123) = (2, 3)$, meaning that second 123 is the second 3 of the minute 2.

Example 3.2. Given a shift $d = 20$, we have that $c^{20}(30) = (0, 10)$, meaning that second 30 is the second 10 of the minute 0.

Requirements (51) and (52) give instructions for converting a second labelling to a minute labelling. These instructions correspond to the following transformations on labellings.

Definition 3.3. Given a minute labelling $M : \mathbf{Z} \to \mathbf{A}$, we define the labelling after applying Requirement (51) as $\mathrm{R51}(M) : \mathbf{Z} \to \mathbf{A}$ defined, for every $i \in \mathbf{Z}$, by:

$$\mathrm{R51}(M)(i) := \begin{cases} \textsc{driving} & \text{if } M(i-1) = M(i+1) = \textsc{driving}, \\ M(i) & \text{otherwise.} \end{cases}$$

Definition 3.4. Given a shift d, a second labelling $S : \mathbf{Z} \to \mathbf{A}$ and a minute labelling $M : \mathbf{Z} \to \mathbf{A}$, we define the labelling after applying Requirement (52) as the minute labelling $\mathrm{R52}(d, S, M) : \mathbf{Z} \to \mathbf{A}$ defined, for every $i \in \mathbf{Z}$, by:

$$\mathrm{R52}(d, S, M)(i) := \begin{cases} M(i) & \text{if } M(i) \neq \textsc{unknown}, \\ A(d, S, i) & \text{otherwise.} \end{cases}$$

where $A(d, S, i)$ is the activity $a \in \mathbf{A}$ such that by $S^{-1}(a) \cap [d + 60i, d + 60i + 60)$ contains the rightmost interval of maximal length.

In other words, $A(d, S, i)$ is the activity a that either contains the longest consecutive interval among all activities, or if there is a tie between two or more, then a has an interval of maximal length that is to the right of that for any other activity.

4 Order of application

This section is devoted to show that the application of Requirement (51) followed by (52), with no further applications, might yield a configuration where (51) is violated as requirement, while on the other hand, the application of (52) followed by (51) is stable: no further applications of either requirement produce any changes.

Definition 4.1. The unknown labelling is the minute labelling $U : \mathbf{Z} \to \mathbf{A}$ such that, for all $i \in \mathbf{Z}$, $U(i) = \textsc{unknown}$.

The algorithm starts as follows: we are given a second labelling S from the tachograph, a shift d given by the calendar that we are using, and the unknown labelling U as a starting minute labelling in which nothing is registered yet.

Now, we can apply R51 and R52 above. It is an easy observation that $\mathrm{R51}(U) = U$, since there is no DRIVING registered yet. We find the following result:

Theorem 4.2. *Let U be the unknown labelling. There are second labellings S and shifts d such that*

$$\mathrm{R52}(d, S, \mathrm{R51}(U)) \neq \mathrm{R51}\left(\mathrm{R52}(d, S, \mathrm{R51}(U))\right),$$

i.e., such that the application of Requirement (51) after the application of Requirements (51) and (52) still changes the minute labelling.

Proof. Consider, for instance, $d = 0$ and

$$S(s) := \begin{cases} \textsc{driving} & \text{if } c_0^0(s) \text{ is even,} \\ \textsc{rest} & \text{otherwise.} \end{cases}$$

In this case, for any $i \in \mathbf{Z}$,

$$\mathrm{R52}(0, S, \mathrm{R51}(U))(i) = \mathrm{R52}(0, S, U)(i) = \begin{cases} \textsc{driving} & \text{if } i \text{ is even,} \\ \textsc{rest} & \text{otherwise,} \end{cases}$$

and $\mathrm{R51}\left(\mathrm{R52}(d, S, \mathrm{R51}(U))\right)(i) = \textsc{driving}$. □

Now, we are going to prove that, once we have applied Requirement (52) followed by (51), the configuration reached is stable: no further applications will produce any changes.

Theorem 4.3. *Let U be the unknown minute labelling, let S be a second labelling and let d be a shift. Then,* $\mathrm{R51}\left(\mathrm{R52}(d,S,U)\right)$ *is stable under applications of* R51 *and* R52*, i.e., the following hold:*

(i) $\mathrm{R51}\Big(\mathrm{R51}\left(\mathrm{R52}(d,S,U)\right)\Big) = \mathrm{R51}\left(\mathrm{R52}(d,S,U)\right)$,

(ii) $\mathrm{R52}\Big(d,S,\mathrm{R51}\left(\mathrm{R52}(d,S,U)\right)\Big) = \mathrm{R51}\left(\mathrm{R52}(d,S,U)\right)$.

Proof. In this proof, let $M_1 = \mathrm{R52}(d,S,U)$ and let $M_2 = \mathrm{R51}\left(\mathrm{R52}(d,S,U)\right)$.

For (i), if $i \in \mathbf{Z}$, by Definition **??** we have:

$$\mathrm{R51}(M_2)(i) := \begin{cases} \textsc{driving} & \text{if } M_2(i-1) = M_2(i+1) = \textsc{driving}, \\ M_2(i) & \text{otherwise.} \end{cases}$$

Hence, the non-trivial case is when $M_2(i-1) = M_2(i+1) = \textsc{driving}$. If $M_2(i) = \textsc{driving}$, then we are done. Assume towards a contradiction that $M_2(i) \neq \textsc{driving}$. Since $M_2 = \mathrm{R51}(M_1)$, we have that $M_1(i) \neq \textsc{driving}$ (because applying R51 never erases DRIVING) and:

$$M_2(i) := \begin{cases} \textsc{driving} & \text{if } M_1(i-1) = M_1(i+1) = \textsc{driving}, \\ M_1(i) & \text{otherwise.} \end{cases}$$

Moreover,

$$\textsc{driving} = M_2(i-1) = \begin{cases} \textsc{driving} & \text{if } M_1(i-2) = M_1(i) = \textsc{driving}, \\ M_1(i-1) & \text{otherwise.} \end{cases}$$

Since $M_1(i) \neq \textsc{driving}$ we are at the bottom case, hence $M_1(i-1) = \textsc{driving}$. By a symmetric argument, $M_1(i+1) = \textsc{driving}$. But then, $M_2(i) = \textsc{driving}$, which is a contradiction.

For (ii), just notice that R52 is the identity over the known part, and the unknown does not change because we keep the same S. □

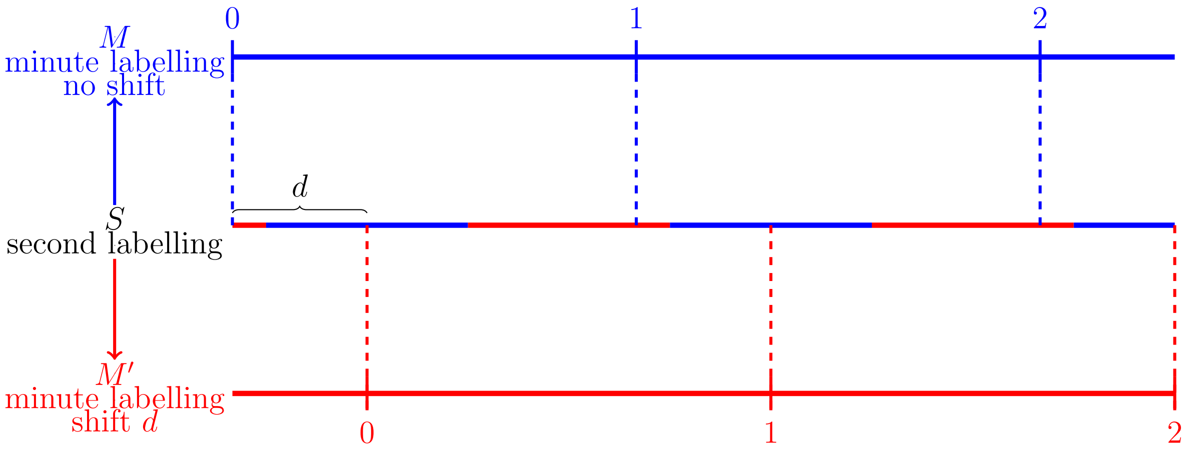

Figure 1: A second labelling S which gives rise to two different minute labellings depending on whether or not a shift d is applied. The top line represents the minute labelling M, the bottom M', and the middle one the second labelling S. The color in the middle line indicates that the second labelling matches with the minute labelling of the respective minute of the same color.

5 Time shifts

In this section we are going to prove that, if we follow Regulation (EU) 2016/799, we obtain that the same sample from the tachograph, interpreted in two calendars with different shifts, can give two completely different minute labellings.

Theorem 5.1. *Let d be a time shift such that $1 \leq d \leq 59$. Let U be the unknown minute labelling and let M and M' be two minute labellings. Then, there exists a second labelling S such that:*

$$\mathrm{R52}(0, S, U) = M \quad \textit{and} \quad \mathrm{R52}(d, S, U) = M'.$$

Proof. We can assume without loss of generality that $d \leq 30$, since otherwise the argument is symmetric. For every $s \in \mathbf{Z}$, we define S as follows:

$$S(s) := \begin{cases} M'(c_0^0(s) - 1) & \text{if } c_1^0(s) = 0, \\ M(c_0^0(s)) & \text{if } 0 < c_1^0(s) \leq 30, \\ M'(c_0^0(s)) & \text{if } c_1^0(s) > 30. \end{cases}$$

Now, notice that:

$$\mathrm{R52}(0, S, U)(i) = A(0, S, i),$$

which is the activity of the longest interval in $[60i, 60i + 60)$. By the definition of S, in that interval there is a first second $60i$ of activity $M'(i - 1)$, then 30 seconds of activity

$M(i)$, and then 29 seconds of activity $M'(i)$. Therefore,

$$\mathrm{R52}(0, S, U)(i) = M(i).$$

Now for the other condition:

$$\mathrm{R52}(d, S, U)(i) = A(d, S, i),$$

which is the activity of the longest interval in $[d + 60i, d + 60i + 60)$. By the definition of S, in that interval there are first $31 - d$ seconds of activity $M(i)$, then 30 seconds of $M'(i)$, and then $d - 1$ seconds of $M(i + 1)$. If $d > 1$, then the activity with the longest interval is $M'(i)$. If $d = 1$, then there is a draw between $M(i)$ and $M'(i)$, but the latest is $M'(i)$. In any case, $\mathrm{R52}(d, S, U)(i) = M'(i)$.

This construction can be visualized in Figure **??**. □

Informally, the theorem says that, given two minute labellings and a shift, there is a second labelling that the driver might have recorded which gives the first minute labelling in one calendar and the second minute labelling in the shifted calendar. In particular, the same activities from a driver can lead, depending on the calendar used, to a minute labelling with only driving or to a minute labelling with only resting.

Requirement (51) does not solve this problem; it only places some mild restrictions on the labellings M, M'. To be precise, these labellings should be feasible in the following sense.

Definition 5.2. A minute labelling $M : \mathbf{Z} \to \mathbf{A}$ is said to be feasible if, for every $i \in \mathbf{Z}$ such that $M(i - 1) = M(i + 1) = \textsc{driving}$, we have that $M(i) = \textsc{driving}$.

It constitutes an easy observation that only feasible minute labellings can be obtained by applying Requirement (51) to minute labellings.

As a direct consequence of the above considerations we obtain the following theorem:

Theorem 5.3. *Let d be a time shift such that $1 \leq d \leq 59$. Let U be the unknown minute labelling and let M and M' be two feasible minute labellings. Then, there exists a second labelling S such that*

$$\mathrm{R51}\left(\mathrm{R52}(0, S, U)\right) = M \quad \textit{and} \quad \mathrm{R51}\left(\mathrm{R52}(d, S, U)\right) = M'.$$

6 Summary of mathematical results

Our mathematical theorems can be summarized as follows:

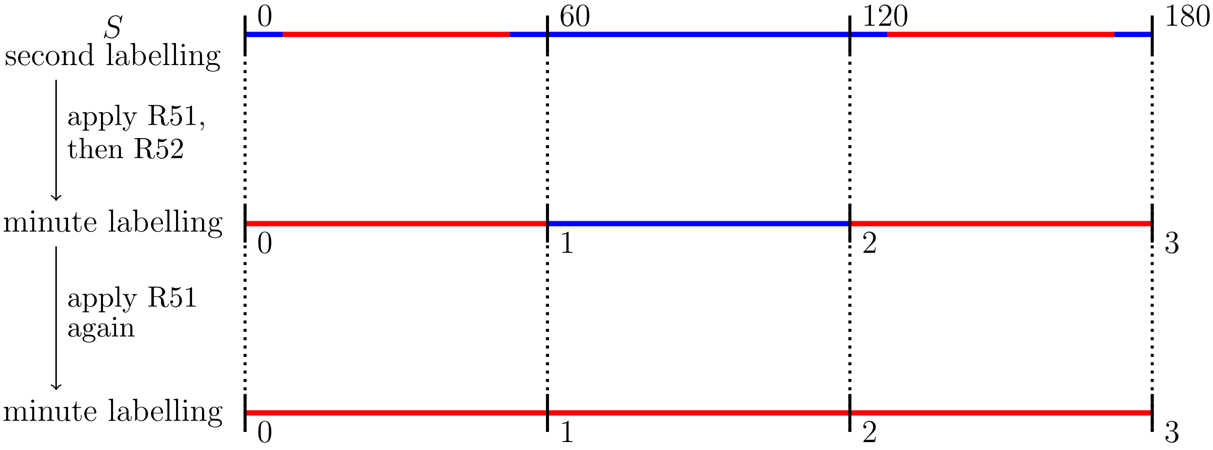

Figure 2: A second labelling that, after applying (51) and (52), can still be changed by applying (51) again. Red represents DRIVING while blue represents REST.

1. Given a second labelling registered by the tachograph:

   - applying Requirement (51) has no effect, since there is no DRIVING activity registered yet;
   - applying Requirement (52) can lead to a configuration which still changes after an application of (51) (see Figure **??**);
   - after applying Requirement (52) followed by (51), the configuration is stable: it does not change under further application of either requirement.

2. Given a second labelling registered by the tachograph and a shift of a few seconds on the calendar:

   - applying Requirement (52) can lead to opposite results among calendars (see Figure **??** and interpret red minutes as DRIVING, blue as REST);
   - after applying all the requirements, these opposite results can persist (Figure **??** is still an example).

7 Experimental results

Since the internal functioning of commercial tachographs is subject to proprietary software restrictions, we cannot freely check the implementation of the regulation that they have chosen. However, Guretruck S.L. has conducted experimental tests and deduce from them that commercial tachographs:

- apply Requirement (52) followed by Requirement (51), which is a dubious interpretation of the law,

- disregard leap seconds, which are part of the UTC time standard prescribed by Regulation (EU) 2016/799.

Guretruck S.L. has conducted experimental tests with real-world driver data as well, finding that the minute labellings computed with proper UTC calendar vary up to an 8% of driving time with respect to the minute labellings computed disregarding leap seconds, even using a small sample of driver files.

8 Conclusions

We have analysed the interdependence between Requirements (51) and (52) of Regulation (EU) 2016/799, giving first some historical notes on the evolution of the text before reaching its current form. We have then exhibited a simple example whereby the application of Requirement (51) followed by (52) leads to a configuration violating Requirement (51). In contrast, we have proved mathematically that an application of Requirement (52) followed by one of Requirement (51) is stable in the sense that the end result is not modified by further applications of either requirement. Experimental examination reveals that industrial tachographs actually implement (52) followed by (51), which is a dubious interpretation of the law but has the technical advantage mentioned above.

We also have studied a situation where the requirements are applied according to two different time standards, where minutes are considered to begin on different calendar seconds. Such a situation arises due to the fact that Regulation (EU) 2016/799 prescribes the use of Coordinated Universal Time UTC —which includes extra *leap* seconds— as time standard, while in practice tachographs disregard leap seconds. We have shown that for any two different time standards, there exists a labelling of second activities such that under one time standard all minutes would be labelled as driving minutes while under the other labelling they would all be labelled as resting minutes. More generally, we have shown that any two feasible minute labellings M and M' may result from the same labelling of seconds given different time standards. We conclude that different time standards, or even the engine being started a few seconds later, may affect whether the activities of a driver will be regarded as illegal.

By analysing real-world data we have checked that differences in driving time may indeed amount up to 8%. Given that drivers can be fined or even imprisoned due to excessive driving times, we consider these differences to be already disastrous.