Abstract: Recent accidents involving autonomous vehicles prompt us to consider how we can engineer an autonomous vehicle which always obeys traffic rules. This is particularly challenging because traffic rules are rarely specified at the level of detail an engineer would expect. Hence, it is nearly impossible to formally monitor behaviours of autonomous vehicles—which are expressed in terms of position, velocity, and acceleration—with respect to the traffic rules—which are expressed by vague concepts such as "maintaining safe distance". We show how we can use the Isabelle theorem prover to do this by first codifying the traffic rules abstractly and then subsequently concretising each atomic proposition in a verified manner. Thanks to Isabelle's code generation, we can generate code which we can use to monitor the compliance of traffic rules formally.

Stichworte: theorem proving, autonomous vehicles, traffic rules, concretisation, linear temporal logic, safe distance