Idle Speed Controller Synthesis Using an Assume–Guarantee Approach

Andrea Balluchi*, Luca Benvenuti§,
Maria Domenica Di Benedetto‡, Alberto L. Sangiovanni–Vincentelli*,†

* PARADES,
Via San Pantaleo, 66, 00186 Roma, Italy
balluchi, alberto@parades.rm.cnr.it

§ Dip. di Informatica e Sistemistica, Università di Roma "La Sapienza",
Via Eudossiana, 18, 00184 Roma, Italy
luca.benvenuti@uniroma1.it

† EECS Dept., University of California at Berkeley,
Berkeley, CA 94720,
alberto@eecs.berkeley.edu

‡ Dip. di Ingegneria Elettrica, Università dell'Aquila,
Poggio di Roio, 67040 L'Aquila, Italy
dibenede@ing.univaq.it

Abstract

The goal of an idle control for automotive engines is to maintain the engine speed within a given range, robustly with respect to load torque disturbances acting on the crankshaft. Mean value models have been used in the past to design idle control algorithms. However, the behavior of the torque generation process and the dynamics of the powertrain are not captured with enough accuracy to guarantee that the idle control specifications as given by car makers are met. We use a cycle-accurate hybrid model to overcome these obstacles. To tackle the complexity of the controller design, the system is decomposed in three parts. For each part in isolation, a control law is derived on a simplified model assuming that the other parts can be controlled to yield appropriate inputs. The overall control strategy is then applied to the system. Hence, the correct interaction of the feedback loops is formally verified using an assume–guarantee approach, to ensure that the behavior of the controlled system meets the given specifications.

1 Introduction

The synthesis of an idle control strategy for an internal combustion engine is among the most challenging problems in engine control. The objective is maintaining the engine speed as close as possible to the value that minimizes fuel consumption, while preventing the engine from stalling. The difficulty lies with the unpredictable load variations coming from the intermittent use of devices powered by the engine, such as the air conditioning system and the steering wheel servo-mechanism. A survey on different engine models and control design methodologies for the idle control is given in Hrovat and Sun (1997). Both time–domain (e.g. Butts et al. (1999)) and crank–angle domain (e.g. Yurkovich and Simpson (1997)) mean–value models have been proposed in the literature. More recently, cycle-accurate models capturing periodic engine speed variations due to torque fluctuations, were investigated in Shim et al. (1996). Multivariable control (Onder and Geering (1993)), ℓ_1 control (Butts et al. (1999)), H_∞ control (Carnevale and Moschetti (1993)), μ-synthesis (Hrovat and Bodenheimer (1993)), sliding mode control (Kjergaard et al. (1994)) and LQ-based optimization (Abate and Di Nunzio (1990)) have been applied to idle control on a variety of models. However, a fully satisfactory solution has still to emerge. In this paper, we use a hybrid model to describe the cyclic behavior of the engine, thus capturing the effect of each spark ignition on the generated torque and the interaction between the discrete torque generation and the continuous power-train and air dynamics. We consider a traditional spark ignition engine without Gas Direct Injection (GDI). The torque generated by each cylinder and applied to the engine crankshaft can be assumed to be a function of the spark ignition time, and of the air-fuel mixture mass loaded in the cylinder during the intake phase. Since the air-to-fuel ratio is assumed to be constant (at the stoichiometric value), then the mixture mass is controlled by the throttle plate position and is subject to the dynamics of the cylinder filling. Hence, the available controls for the idle problem are: the spark ignition time and the position of the throttle valve, which regulates the air inflow[1]. A hybrid model of the plant is obtained from the general model of an internal combustion engine presented in reference Balluchi et al. (2000b), by using

[1] The effect of a spark command on the torque generation is "stronger" than the one of a throttle plate command, since air inflow is subject to both manifold dynamics and delay due to mix compression. Hence, sudden loads can be much better compensated with spark ignition than with air inflow, while air inflow can be used to control the engine in steady state.

nonlinear expressions and model parameters identified on a commercial car in collaboration with our industrial partner, Magneti Marelli Powertrain S.p.A. . In Balluchi et al. (2000b) and Balluchi et al. (2000a), the problem of maintaining the crankshaft speed within a given range was formalized as a "safety" specification for the hybrid closed–loop system[2]. For a simplified engine hybrid model, where some nonlinear expressions were linearized and no actuation delay was considered, the idle control problem was solved by computing analytically the set of all hybrid states for which there exists a hybrid control strategy meeting the specification. The class of all "safe" controllers obtained by the procedure was called the *maximal controller*. Despite the simplification of the model, the expression of the maximal controller obtained in Balluchi et al. (2000b), Balluchi et al. (2000a) is quite complex. Consequently, the implementation of a particular controller extracted from the maximal controller is quite expensive in terms of computing time and memory.

To solve the problem in ways that are industrially feasible, we have to take into account nonlinearities, actuation delays and yet we have to keep a close look at implementation costs. The approach we propose in this paper is to select semi-heuristically an easy–to–implement controller and then verify that it satisfies the specifications.

Verifying the system by simulation and prototyping is certainly possible but we cannot guarantee that the system will satisfy the specifications in all operating conditions. In fact, it is often the case that idle control needs extensive empirical adjustments in the car.

In this paper, we present a first cut for a methodology based on a divide and conquer approach to obtain the controller and formal techniques to guarantee that the controller is contained in the maximal controller and, hence, it satisfies the specifications.

In our case, the closed–loop system is viewed as composed of three sub-systems (intake manifold, cylinders and powertrain sub-systems). The control law is derived by simplifying substantially each of the subsystems so that the hybrid nature of the model is ignored and the subsystems are linearized and discretized with a fixed sampling time. The control law is synthesized so that the constraints are satisfied in this simplified domain. Then, this control law is applied to the full-fledged system. Of course, at this point, there is no *guarantee* that the control law will yield a closed–loop system that satisfies the constraints even though the decomposition and the corresponding simplifications have

[2]A safety specification requires the system to stay within a set of specified safe states.

been made so that we do not wander far from the original model. The basic idea of our methodology is to verify each sub-system in isolation assuming that the behavior of the other sub-systems satisfies an appropriate set of conditions. Then, the consistency of the assumptions on the behaviors is verified, knowing that each of the sub-systems works correctly in isolation. The sub-systems are the same as the ones identified for the derivation of the control law. However, the behavior of the closed-loop power-train sub-system is still too complex to verify formally, since it contains the hybrid powertrain model. Hence, the hybrid powertrain model is decomposed itself in the continuous part and the discrete part and verified following the same divide and conquer approach. Note that this approach is a particular case of the assume–guarantee paradigm widely used in formal verification.

To summarize, our methodology consists of dividing the overall system in a set of interconnected sub-systems, simplifying the model for each, derive a control law for the decomposed, simplified system and finally formally verify that the control law (possibly modified to take into account some of the simplifications made) satisfies the constraints of the full fledged model. To the best of our knowledge, this approach is novel in hybrid control.

The paper is organized as follows: in Section 2, a description of the hybrid model of the engine in the idle region of operation is recalled. In Section 3, an idle speed controller is proposed and in Section 4, the verification results on the behavior of the closed–loop hybrid system are reported.

2 Plant hybrid model

In this section we briefly describe a hybrid model of a 4–stroke internal combustion engine. This model has been obtained from the hybrid model presented in reference Balluchi et al. (2000b), by specifying nonlinear expressions and model parameters on the bases of the experimental data obtained from a commercial car at idle speed provided us by Magneti Marelli Powertrain (Italy).

The model is composed of four interacting blocks, namely, the intake manifold, the cylinders, the power-train and the actuators, as shown in figure 1.

The **intake manifold** pressure dynamics is a continuous-time process controlled by the throttle-valve position α. Denoting by p the pres-

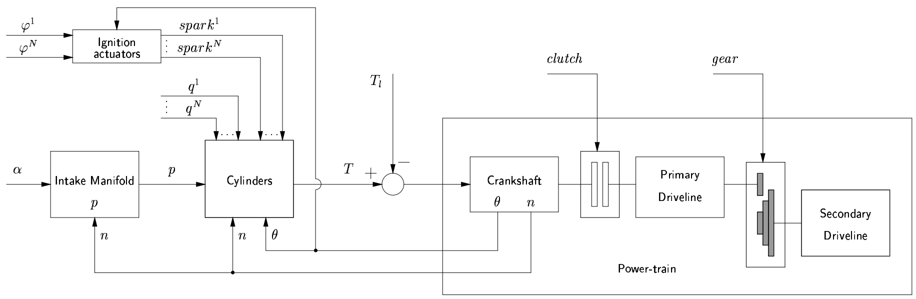

Figure 1: Model of the engine.

sure, manifold dynamics is modelled as

$$\dot{p}(t) \quad = \quad a_p(p(t))\, p(t) + b_p(p(t))\, s(\alpha(t)) \tag{1}$$

where $s(\alpha)$ is the *equivalent throttle area*, given in terms of throttle angle α. Parameters a_p and b_p depend in a strongly nonlinear fashion on the geometric characteristics of the manifold, on the physical characteristics of the gas and atmosphere, and on the current value of the pressure p. The dynamics of actuation of the throttle valve is modelled by a linear first–order dynamical system:

$$\dot{\alpha}(t) \quad = \quad a_\alpha \alpha(t) + b_\alpha V(t) \tag{2}$$

where V is the motor input voltage that is assumed to be a discrete time signal produced with a sampling period τ_A.

The **cylinders** block models the torque generation. The torque T generated by each piston at each cycle depends on the thermodynamics of the air–fuel mixture combustion process. The profile of T depends on the phase of the cylinder, the piston position, the mass m of air and q of fuel loaded during the intake phase, and on the spark ignition timing. For idle speed values, the quantity m of air loaded into each cylinder at the end of the intake run can be assumed to depend only on the value of the intake manifold pressure at the intake end time t_{int} as

$$m \quad = \quad k_m(p(t_{int}))\, p(t_{int}) \tag{3}$$

Assuming that fuel injection is regulated by an inner control loop that maintains the air-to-fuel ratio to stoichiometry, the profile of the torque T generated by each cylinder can be described by a piecewise constant function that is assumed to be zero everywhere except in the expansion phase in which

$$T(t) \quad = \quad G\, m\, \eta(\varphi) \tag{4}$$

where the gain G is a constant parameter, φ is the spark advance[3], and $\eta(\varphi)$ is the ignition efficiency.

When the gear is neutral and the clutch is released, the secondary driveline is disconnected from the engine so that the **power-train** is described only in terms of the crankshaft speed n and position θ, by the continuous time system

$$\dot{n}(t) = a_n\, n(t) + b_n\,(T(t) - T_l(t)) \quad (5)$$
$$\dot{\theta}(t) = k_n\, n(t) \quad (6)$$

where a_n, b_n are constant parameters, T is the torque produced by the engine, and T_l represents a load torque acting on the crankshaft.

The ignition **actuators** must produce the spark ignition at every cycle, according to the current decision of the control algorithm, and synchronously with the crankshaft position θ. Since ignition control takes time to actuate, then, it has to be decided sufficiently in advance to make sure that it is properly delivered to the plant. The spark is in general ignited with a different spark advance at every cycle. The value of the spark advance must then be computed at the end of the intake stroke, so that the ignition subsystem can be programmed to ignite the spark at the proper time.

In conclusion, the behavior of a four–cylinder in-line engine and power-train can be represented using only one discrete state, as shown in figure 2. In fact, the engine kinematics are such that, at any time, each cylinder is in a different stroke of the engine cycle and only one cylinder is generating the torque T. Every half of a crankshaft run, i.e., when $\theta = 180$, the control law $f_\varphi(\cdot)$ is computed to obtain the spark ignition to be applied to the cylinder that is entering the compression stroke at the current dead center. The throttle valve control $f_\alpha(\cdot)$ is computed at fixed frequency $1/\tau_A$ and will affect the amount of air loaded by the cylinder that is performing the intake stroke at the current sampling time. The torque $T - T_l$ is the total torque acting on the crankshaft.

3 Idle speed control design

The specification for the idle speed control is to maintain the crankshaft revolution speed around a nominal value n_0, so that it never exits a range $n_0 \pm \Delta n$, with $\Delta n > 0$. This specification has to be achieved for

[3]The spark ignition time is commonly defined in terms of the spark advance that denotes the difference between the angle of the crankshaft when the cylinder is at the end of the compression stroke and the one at the time of ignition.

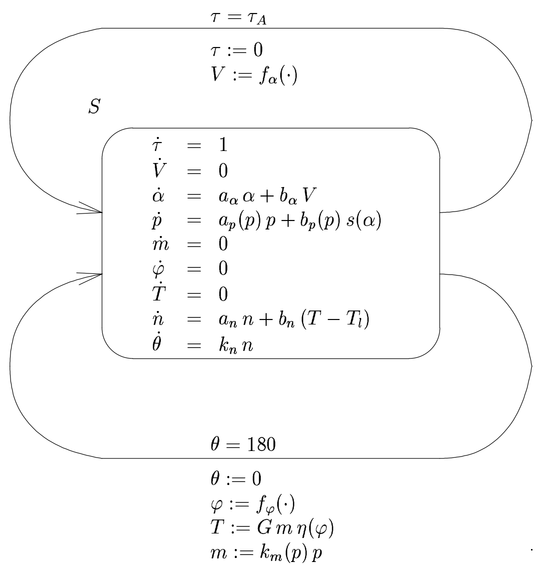

Figure 2: Engine hybrid model at idle speed.

any value of the load torque disturbance T_l within a lower bound zero and an upper bound $T_l^M > 0$.

The proposed control is a state feedback control. While the spark advance feedback $f_\varphi(\cdot)$ is computed at dead–center times, the throttle feedback $f_\alpha(\cdot)$ is set at fixed–frequency sampling times.

Let $\{t_i\}$ denote the sequence of dead–center times and let t_i denote the current dead–center time.

According to the engine hybrid model described in the previous section and shown in figure 2, the spark advance control $\varphi(t_i)$, chosen at time t_i, will affect the value of the torque $T(t_{i+1})$ that drives the crankshaft from time t_{i+1} to time t_{i+2}. The amount of driving torque $T(t_{i+1})$ depends also on the value of the load disturbance $T_l(t)$, acting on the same time interval $[t_{i+1}, t_{i+2})$. The result of the action of this torque will be a given value of crankshaft speed $n(t_{i+2})$ at time t_{i+2}. Let $\{t_j^A\}$ denote the sequence of sampling times t_j^A of the throttle valve control feedback $f_\alpha(\cdot)$. The control actions $\alpha(t_j^A)$ for $t_j^A \in [t_i, t_{i+1})$ drive the manifold dynamics during an intake stroke starting from the dead–center time t_i to the dead–center time t_{i+1}. The amount of mass loaded by the cylinder at time t_{i+1} depends on these control actions. Note that the corresponding torque will be produced only from time t_{i+2} to time t_{i+3}, due to the delay introduced by the compression stroke.

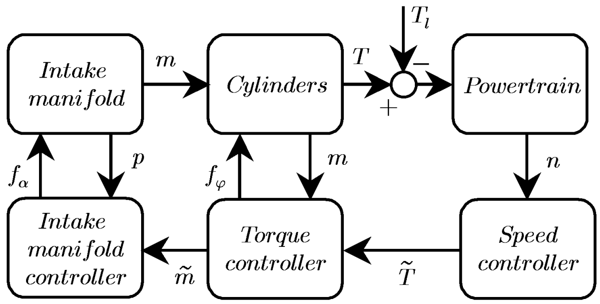

Figure 3: Control scheme.

3.1 Controller structure

Due to the complexity of the system to control, our strategy is to decompose the system into three nested sub-systems and to devise an appropriate control for each of them in isolation, assuming that the variables that connect the sub-system to the others satisfy an appropriate assumption. The interconnect variables are subject to control and the assumption is chosen so that the controller can indeed make them true when applied to the appropriate sub-system. Of course, there is no a priori guarantee that the control law derived with these heuristics satisfy the constraints when applied to the hybrid model. The goal of the verification step is to prove that the strategy pays off: the constraints are indeed satisfied.

The controller is composed of three nested loops:

- an engine speed control in the outer loop, which is responsible for the generation of torque values the cylinders are requested to produce;
- a torque control in the middle loop, which regulates the torque produced by the engine to the desired value and is implemented by the spark advance feedback $f_\varphi(\cdot)$;
- a manifold control in the inner loop, which is responsible for regulation of the mass loaded by the cylinders and implemented by the throttle valve feedback $f_\alpha(\cdot)$.

The overall control scheme is shown in figure 3.

3.2 Speed and torque control loops

In this section, we detail the simplifications and show how the control law is derived. The hybrid nature of the torque generation process is approximated by means of a fixed frequency $n_0/30 = 1/\tau_0$ dicrete time process and the driveline dynamics is discretized with sampling period τ_0 so that it reduces to:

$$n(k\tau_0 + \tau_0) = a_n^d n(k\tau_0) + b_n^d \left(T(k\tau_0) - T_l(k\tau_0)\right)$$

with $a_n^d = e^{a_n \tau_0}$ and $b_n^d = (e^{a_n \tau_0)} - 1)(b_n/a_n)$. The robustness of the closed–loop system behavior with respect to this approximation has to be checked in the verification phase. Moreover, assuming that the middle loop will be able to produce the requested torque with a one-step delay, we have

$$T(k\tau_0) = \widetilde{T}(k\tau_0 - \tau_0) \tag{7}$$

where $T(k\tau_0)$ is the driving torque during the expansion phase from time $k\tau_0$ to $k\tau_0 + \tau_0$ and $\widetilde{T}(k\tau_0 - \tau_0)$ is the reference torque computed at the end of the intake phase by the speed controller. This torque depends on the mass of air

$$m(k\tau_0 - \tau_0) = k_m(p(k\tau_0 - \tau_0))\ p(k\tau_0 - \tau_0)$$

loaded in the cylinder entering the compression phase and on the spark advance $\varphi(k\tau_0 - \tau_0)$ that will be applied to the same cylinder.

We design an engine speed control feedback such that the torque $\widetilde{T}(k\tau_0 - \tau_0)$ emulates that of a PI controller, represented as follows:

$$\widetilde{T}(z) = K_p \left(1 + \frac{\tau_0 z}{\tau_I (z-1)}\right) \left(n(z) - n_0 \frac{z}{z-1}\right) \tag{8}$$

This controller is able to asymptotically compensate constant torque disturbances. The gain K_p and the time constant τ_I are selected as to stabilize the system dynamics

$$n(k\tau_0 + \tau_0) = a_n^d n(k\tau_0) + b_n^d \widetilde{T}(k\tau_0 - \tau_0) \tag{9}$$

around the nominal engine speed n_0, when the disturbance torque T_l is constant.

The spark advance is then computed by simply inverting equation

$$\widetilde{T}(k\tau_0 - \tau_0) = G\ m(k\tau_0 - \tau_0))\ \eta\left(\varphi(k\tau_0 - \tau_0)\right)$$

taking into account the saturation $\varphi \in [\varphi_{min}, \varphi_{max}]$. If the computed spark advance is not saturated, then it will be able to produce the desired torque, as in (7), on the basis of the mass of air loaded at time $k\tau_0 - \tau_0$.

Furthermore, the middle–loop control has to generate the sequence of reference values $\widetilde{m}(k\tau_0 - \tau_0)$ that is given as input to the manifold control inner loop. This reference value, when produced, will affect the torque generated in the time interval $[k\tau_0+\tau_0, k\tau_0+2\tau_0]$ and is computed by inverting equation

$$\widetilde{T}(k\tau_0 - \tau_0) = G\ \tilde{m}(k\tau_0 - \tau_0)\ \eta\,(\varphi_0) \tag{10}$$

where the parameter φ_0, with $\varphi_{min} < \varphi_0 < \varphi_{max}$, is the nominal spark advance to be used during idle control. The tuning of the control parameter φ_0 to value smaller than φ_{max} allows some degree of reacting to fast positive torque requests using the spark advance input. Similarly, setting φ_0 to a value greater than φ_{min}, allows to react to fast negative torque requests.

Note that the mass of air loaded into the cylinder at time $k\tau_0-\tau_0$, i.e., at the end of the intake phase, depends on the throttle control applied on the time interval $[k\tau_0 - 2\tau_0, k\tau_0 - \tau_0]$.

3.3 Intake manifold control loop

The objective of the intake manifold control is that of making the cylinders load the amount of mass $\widetilde{m}$ specified by the torque control.

For the design of the intake manifold control, we assume that the reference signal $\widetilde{m}$ is produced at a fixed frequency $1/\tau_0$ and τ_A is such that $\tau_0 = N_A\tau_A$ for an appropriate integer N_A . The robustness of the closed–loop system with respect to this assumption has to be checked in the verification phase.

The intake manifold and cylinder filling dynamics are discretized with sampling period equal to the throttle valve control sampling time τ_A. By inverting equation (3), a sequence $\tilde{p}$ of manifold pressure set-points is obtained from the sequence of desired mass $\widetilde{m}$ given by (10). Hence, a PID controller that produces convergence of the manifold pressure p to the target signal $\tilde{p}$ is used for the throttle piecewise–constant control feedback $f_\alpha(\cdot)$:

$$V(z)=\hat{K}_p\left(1+\frac{\tau_A z}{\hat{\tau}_I(z-1)}+\frac{\hat{\tau}_D(z-1)}{\tau_A z}\right)(p(z)-\tilde{p}(z)) \tag{11}$$

3.4 Simulations

Simulation results are reported in figure 4. The crankshaft revolution speed has to be maintained around the nominal value $n_0 = 800$ rpm

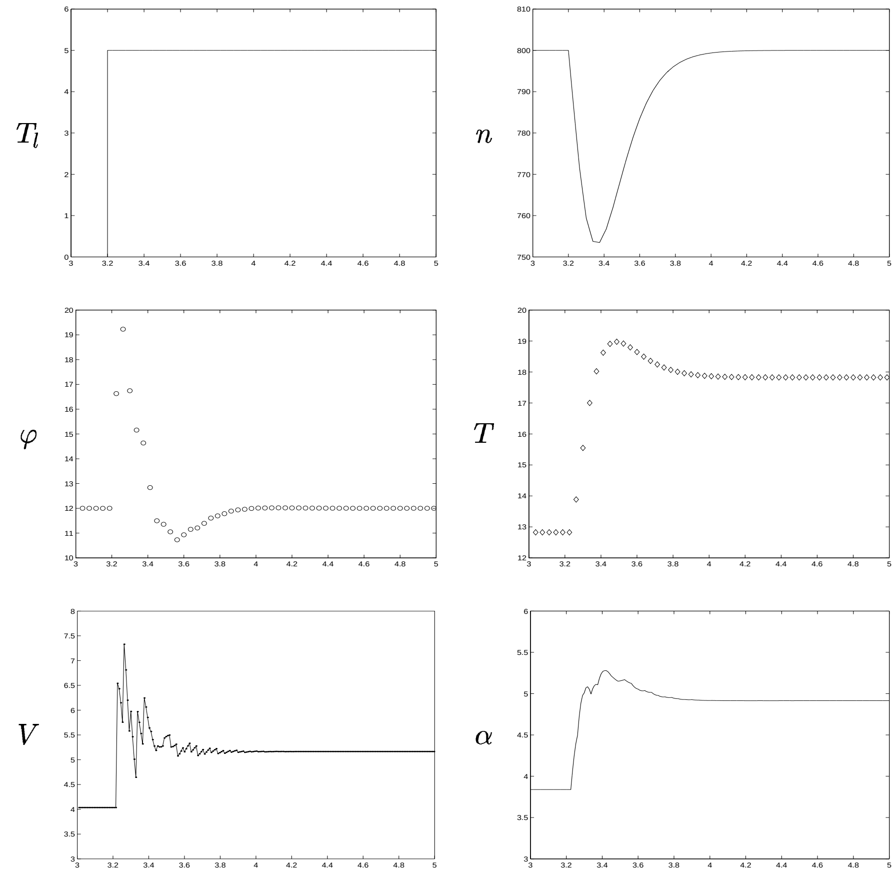

Figure 4: Simulation results.

with maximum excursion of ± 50 rpm so that $\tau_0 = 30/n_0 = 37.5$ msec. The value of the powertrain parameters are $a_n = -1.531$ and $b_n = 95.49$; those of the intake manifold are: $\tau_A = \tau_0/4$, $a_p = -20.94$, $b_p = 1821$, $a_\alpha = -10.3$, $b_\alpha = 9.8$ and $\varphi_0 = 12$. Finally, the PID controllers are defined by the following time constants and gains: $K_p = 0.0781$, $\tau_I = 234.5$ msec, $\hat{K}_p = 0.0613$, $\hat{\tau}_I = 135.7$ msec, $\hat{\tau}_D = 29.5$ msec. Figure 4 shows relevant signals in a simulation of the closed–loop system, obtained with a load torque T_l that is a step of amplitude 5 Nm applied at time $t = 3.2$ sec.

4 Closed–loop system behavior verification

In this section, we need to show that the hybrid feedbacks described in sections 3.2, 3.3, when applied to the full hybrid system model described in section 2, achieve the task of maintaining the engine speed within the specified range, for any action of the load disturbance, provided that the initial condition of the hybrid system belongs to a specified set. In other words, we need to show that a given set of initial conditions is a robust invariant set for the closed loop system obtained by applying the proposed idle speed control to the hybrid engine model. This result guarantees that, if the hybrid system state is steered inside this set (that may not be the maximal one), then the proposed idle feedback control can be activated and the idle speed specification will be met under any load disturbance.

In Balluchi et al. (2000a), the maximal robust invariant set for an engine at idle speed was computed analytically for a simplified engine hybrid model, where the nonlinear expressions were linearized and no actuation delays were considered. The main objective there was to establish the best performances achievable by a given engine without adding any detail and/or constraints on the idle speed controller. The approximated linear expressions were used to make the analytical computation feasible and the largest set of initial conditions for which at least an idle speed controller exists was derived.

In this paper, we added details and constraints on the controller, specifying actuator delays and dynamics in the hybrid model of the engine. Hence, the verification task is more complex and cannot be carried out analytically. We need to show that, from a given set of initial conditions, the controller synthesized in the previous section achieves the idle speed specification. Due to the added details on actuations characteristics and due to the choice of a particular controller, this set of initial conditions will be necessarily contained in the maximal robust invariant set for idle speed control computed for the nonlinear model.

Performing formal verification of the behavior of the entire hybrid closed–loop system with respect to the given specification is prohibitively complex. Hence, we decided to apply an assume–guarantee paradigm to verify the correctness of the proposed controller. The verification is based on the same decomposition of the system used in the design of the feedback controls. Then, we consider first the powertrain closed–loop system, then the cylinders closed–loop system, and finally the intake manifold closed–loop system.

4.1 Engine speed feedback formal verification

Applying the assume–guarantee paradigm, the correctness of the behavior of the speed control outer loop is verified *assuming that the torque control middle loop will produce the requested values of torque with a single phase delay.*

First, we analyze the evolution of the continuous dynamics (5)-(6). To this end, we compute in the configuration subspace (n, T) a set $\mathcal{P}$ such that if, at each dead center, the configuration is inside the set $\mathcal{P}$, then the continuous evolution of $n(t)$ will satisfy the system specification $n(t) \in [n_0 - \Delta, n_0 + \Delta]$ also for any t between dead center times, under any action of the torque disturbance T_l. The set $\mathcal{P}$ is obtained by backwards integration of equations (5)-(6) over a stroke for $T_l \in [0, 5]Nm$. Figure 5 shows the set $\mathcal{P}$.

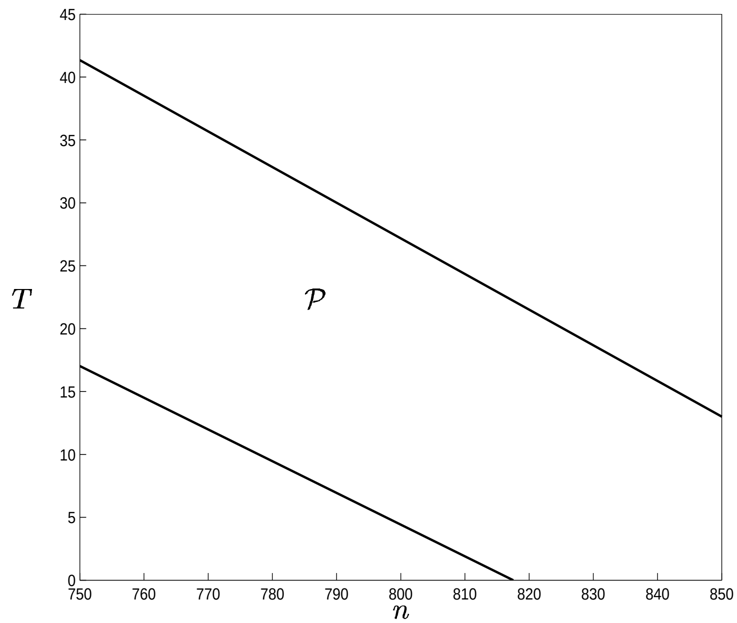

Figure 5: The set $\mathcal{P}$.

Hence, the speed controller produces a correct behavior if, for any evolution of the closed–loop system, at each dead center the engine torque T and the engine speed n belong to the set $\mathcal{P}$. Let z_k^I denote the state of the PI engine speed controller. Under the assumption that the torque control middle loop will produce the requested values of torque with a single phase delay, the evolution of variables (n_k, T_k, z_k^I) for the

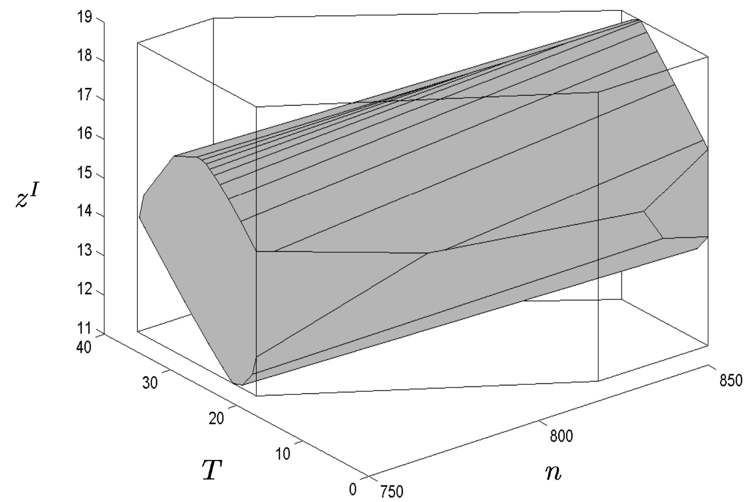

Figure 6: Maximal invariant set $\mathcal{M}_{\mathcal{P}}$ contained in $\mathcal{P} \times \mathbb{R}$, robust with respect to the load torque disturbance T_l.

closed–loop system[4] is given by

$$n_{k+1} = e^{a_n t^\star} n_k + \frac{b_n}{a_n}(e^{a_n t^\star} - 1)(T_k - T_l) \qquad (12)$$

$$T_{k+1} = \widetilde{T}_k = z_k^I - K_P \frac{\tau_I + \tau_0}{\tau_I}(n_k - n_0) \qquad (13)$$

$$z_{k+1}^I = z_k^I - K_P \frac{\tau_0}{\tau_I}(n_k - n_0)\ . \qquad (14)$$

In (12), $t^\star$ denotes the dead-center time that is modeled as a bounded unknown disturbance in the range $[30/(n_0 + \Delta), 30/(n_0 - \Delta)]$. This formalization allows us to verify the robustness of the closed–loop system with respect to the fact that the engine speed controller is designed for the discrete time approximation of the process (5) using $t^\star = \tau_0$. At each dead center the engine torque T_k and the engine speed n_k belong to the set $\mathcal{P}$, if there exists a not empty robust invariant set $\mathcal{M}_{\mathcal{P}}$ contained in $\mathcal{P} \times \mathbb{R}$ and the PI controller initial configuration z_0^I is chosen such that $(n_0, T_0, z_0^I) \in \mathcal{M}_{\mathcal{P}}$.

Then, to complete the verification of the speed controller we have

[4]The index k refers to the k-th dead center.

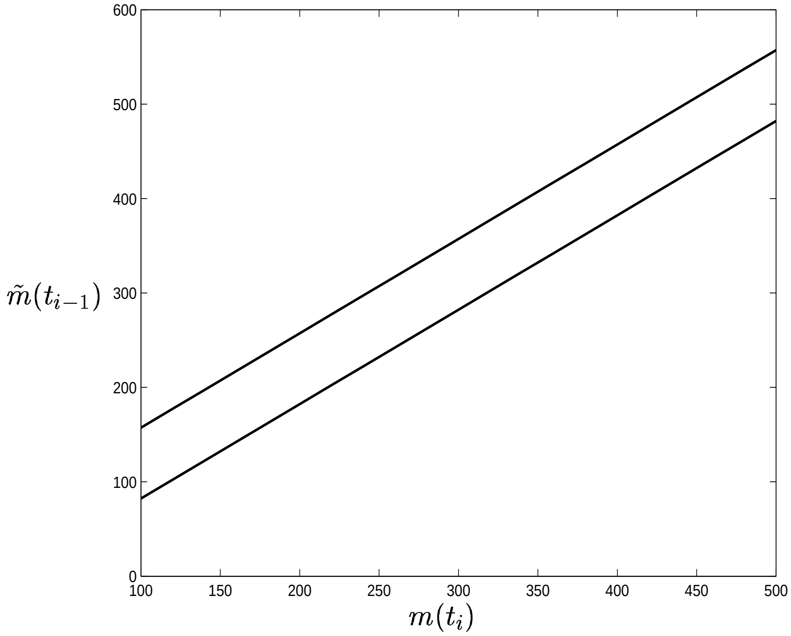

Figure 7: Assumed behavior for the intake manifold closed–loop subsystem.

to compute a robust invariant set $\mathcal{M}_{\mathcal{P}}$ for dynamics (12),(13) and (14), contained in $\mathcal{P} \times \mathbb{R}$. Such invariant set is required to be robust with respect to both the unknown load torque T_l and the unknown dead center times $t^\star$.

Figure 6 shows the maximal invariant set $\mathcal{M}_{\mathcal{P}}$ for dynamics (12),(13) and (14) contained in $\mathcal{P} \times \mathbb{R}$, robust with respect to the load torque disturbance T_l only. This set has been computed applying backwards reachability analysis starting from the set $\mathcal{P} \times \mathbb{R}$ under any action of the disturbance T_l.

Further elaboration of this set to ensure robustness with respect to the disturbance $t^\star$ is currently under investigation.

Notice that, since the assumed behavior for the torque closed–loop sub-system is that of producing the desired torque $\tilde{T}$ with a single phase delay, the specification to be verified for the middle sub-system does not depend on the evolution of the outer control loop. This allows us to formally verify that if the intake manifold control inner loop will exhibit an input-output behavior that is contained in the stream depicted in figure 7, in terms of requested mass $\widetilde{m}(k-1)$ and loaded mass during the intake strokes $m(k)$, then the torque control middle loop is able to produce the requested behavior between the desired torque $\tilde{T}$ and the engine torque T.

Finally, in the last step of the assume-guarantee approach, we will consider the verification of the intake manifold control inner loop to show that the behavior of the throttle valve control is correct, in the sense that it provides the assumed behavior specified in figure 7. An objective of this verification is to show that the discrete representation of the pressure dynamics, used in the design of the throttle valve control, models sufficiently well the continuous evolution of the manifold pressure. A second issue is verifying that the interaction between the two loops with different triggers (the throttle control running at fixed frequency $1/\tau^A$ and torque control synchronized with the engine dead centers) produces a correct behavior.

5 Conclusions

The idle speed control problem has been formalized as a safety specification for a hybrid model of the engine and the power-train. The hybrid model describes the intake manifold and cylinder filling dynamics, the torque generation process and the powertrain, as well as throttle and spark ignition actuators. An idle speed controller has been designed exploiting the decomposition of the system in three components: the engine speed controller, the torque controller and the intake manifold controller. For the design of each controller, a simplified model of the plant is used. Each controller is synthesized assuming that the other sub-systems can be controlled to give the appropriate input-output behavior.

The control law so obtained is then applied to the hybrid system modeled in its entirety and simulation results are obtained. Since there is no guarantee that the behavior of the closed–loop system will satisfy the specifications, we apply formal verification techniques to demonstrate that the control law does indeed meet the constraints. Since formal verification is a very complex task, we applied an assume–guarantee approach that views the system as composed of the three sub-systems for which the control law was derived. The assume–guarantee principle allows us to obtain a set of formal verification problems that are solvable within the domain of present formal verification tools.

References

Abate, M. and Di Nunzio, V. (1990). Idle speed control using optimal regulation. Technical Report 905008, SAE.

Balluchi, A., Benvenuti, L., Di Benedetto, M. D., Miconi, G. M., Pozzi, U., Villa, T., Wong-Toi, H., and Sangiovanni-Vincentelli, A. L. (2000a). Maximal safe set computation for idle speed control of an automotive engine. In Lynch, N. and Krogh, B. H., editors, *Hybrid Systems: Computation and Control*, volume 1790 of *Lecture Notes in Computer Science*, pages 32–44. Springer-Verlag, New York, U.S.A.

Balluchi, A., Benvenuti, L., Di Benedetto, M. D., Pinello, C., and Sangiovanni-Vincentelli, A. L. (2000b). Automotive engine control and hybrid systems: Challenges and opportunities. *Proceedings of the IEEE*, 88, "Special Issue on Hybrid Systems" (invited paper)(7):888–912.

Butts, K. R., Sivashankar, N., and Sun, J. (1999). Application of ℓ_1 optimal control to the engine idle speed control problem. *IEEE Trans. on Control Systems Technology*, 7(2):258–270.

Carnevale, C. and Moschetti, A. (1993). Idle speed control with H_∞ technique. Technical Report 930770, SAE.

Hrovat, D. and Bodenheimer, B. (1993). Robust automotive idle speed control design based on μ-synthesis. In *Proc. IEEE American Control Conference*, pages 1778–1783, S. Francisco, CA.

Hrovat, D. and Sun, J. (1997). Models and control methodologies for IC engine idle speed control design. *Control Engineering Practice*, 5(8).

Kjergaard, L., Nielsen, S., Vesterholm, T., and Hendricks, E. (1994). Advanced nonlinear engine idle speed control systems. Technical Report 940974, SAE.

Onder, C. H. and Geering, H. P. (1993). Model-based multivariable speed and air-to-fuel ratio control of a SI engine. Technical Report 930859, SAE.

Shim, D., Park, J., Khargonekar, P. P., and Ribbens, W. B. (1996). Reducing automotive engine speed fluctuation at idle. *IEEE Trans. on Control Systems Technology*, 4(4):404–410.

Yurkovich, S. and Simpson, M. (1997). Crank-angle domain modeling and control for idle speed. *SAE Journal of Engines*, 106(970027):34–41.