EPiC Series in Computing

Volume 48, 2017, Pages 75–91

ARCH17. 4th International Workshop on Applied Verification of Continuous and Hybrid Systems

Formal Verification of a Multi-Basal Insulin Infusion Control Model.

Xin Chen, Souradeep Dutta, and Sriram Sankaranarayanan

University of Colorado Boulder, CO

Abstract

The artificial pancreas concept automates the delivery of insulin to patients with type-1 diabetes, sensing the blood glucose levels through a continuous glucose monitor (CGM) and using an insulin infusion pump to deliver insulin. Formally verifying control algorithms against physiological models of the patient is an important challenge. In this paper, we present a case study of a simple hybrid multi-basal control system that switches to different preset insulin delivery rates over various ranges of blood glucose levels. We use the Dalla-Man model for modeling the physiology of the patient and a hybrid automaton model of the controller. First, we reduce the problem state space and replace nonpolynomial terms by approximations with very small errors in order to simplify the model. Nevertheless, the model still remains nonlinear with up to 9 state variables.

Reachability analysis on this hybrid model is used to verify that the blood glucose levels remain within a safe range overnight. This poses challenges, including (a) the model exhibits many discrete jumps in a relatively small time interval, and (b) the entire time horizon corresponding to a full night is 720 minutes, wherein the controller time period is 5 minutes. To overcome these difficulties, we propose methods to effectively handle time-triggered jumps and merge flowpipes over the same time interval. The evaluation shows that the performance can be improved with the new techniques.

1 Introduction

The artificial pancreas concept refers to a series of increasingly sophisticated devices that automate the delivery of insulin to patients with type-1 diabetes in a closed loop, automatically responding to changes in the patient's blood glucose levels and activities such as meals and exercise [29, 16, 34]. Currently, patients self-regulate their own insulin delivery in response to their blood glucose levels measured through a "finger-stick" blood glucose meter or a continuous glucose monitor [47, 9]. Short-term risks include extremely low blood glucose levels called *hypoglycemia*, technically defined as blood glucose levels below 70 `mg/dl` and high blood glucose levels called *hyperglycemia* that occur when blood glucose levels are above 180 `mg/dl`. Hypoglycemia can lead to seizures, loss of consciousness, coma or even death in extreme cases. Extreme hyperglycemia involving blood glucose levels consistently higher than 300 `mg/dl` can lead to a dangerous condition called ketoacidosis. Long term risks of elevated blood glucose levels include widespread damage to critical organs such as kidneys, heart and the nervous system. As a result, the need to maintain blood glucose levels inside a relatively narrow range

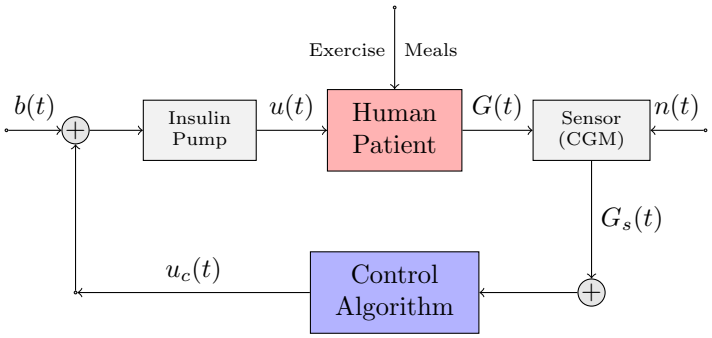

Figure 1: Overview of the key components of an artificial pancreas control system. $b(t)$: external user commanded insulin, $u(t)$: insulin infused to patient, $G(t)$: blood glucose level of the patient, $n(t)$: sensor measurement error (noise), $G_s(t)$: glucose level estimated/reported by sensor, $u_c(t)$: insulin infusion commanded by the algorithm.

requires the patients to periodically monitor their blood glucose levels and adjust their insulin dosages [9]. This can be complicated during night time when the patient is asleep, during meal times when the patient ingests significant amounts of carbohydrates, and during strenuous exercise.

Figure 1 shows the overall closed loop at a glance. Typical artificial pancreas systems use continuous glucose monitors to measure blood glucose levels periodically, and insulin pumps to deliver artificial insulin analogs at precisely programmable rates over time. To close the loop, a control algorithm uses the sensor readings to automatically decide the future insulin delivery. The design of control algorithms is complicated by many factors including (a) the presence of large unanticipated disturbances such as meals and exercise, (b) the action profile of insulin has delays including peak action two hours after infusion and persistence up to 7 hours. Thus, insulin delivered at any point in time incurs a nontrivial delay before it begins to act, and will continue to act long after it is potentially "needed", and (c) the continuous glucose monitors are noisy and prone to systematic errors including dropouts and pressure induced sensor attenuation [22]. These errors affect the insulin dosing decisions made by the algorithm.

At the same time, the artificial pancreas is safety critical. Excess insulin delivered to the patient can carry with it severe risks associated with hypoglycemia. On the other hand, insufficient insulin delivery can lead to elevated glucose levels for long periods of time, risking longer term consequences to the patient.

Closed-loop functional verification seeks to verify that the closed loop formed by the composition of the software with the glucose sensors, insulin pump and the patient satisfies important safety and liveness properties. Safety properties include "the user will not experience extremely high ($G \geq 300$`mg/dl`) or low ($G \leq 70$`mg/dl`) levels of blood glucose under an assumed set of meal behaviors". The properties in question can involve real-time liveness properties as well. For example, "If the blood glucose level falls continuously for at least 30 minutes and the blood glucose level is less than 180 `mg/dl`, then the pump should be shut off".

In this paper, we present the Dalla-Man et al. model for human insulin glucose regulation and a simple *multiple basal* control system. We present some safety properties of the system. Next, we use the Flow* tool to perform a reachability analysis of the resulting closed loop.

Table 1: An overview of selected differential equation-based modeling approaches for human insulin-glucose regulation.

Model Name	Vars	Remarks
Bergman	3	2 insulin + 1 glucose compartment [3, 4]
Li (DDE)	2	1 insulin + 1 glucose compartment [35, 32] delays between glucose bolus and insulin response.
Cobelli	11	Comprehensive model including glucagon and renal function submodels [15, 17].
Sorensen	19	Comprehensive model with brain, vascular, and renal submodels [48].
Hovorka	11	Comprehensive model with brain, endogenous glucose and renal submodels [28, 27, 53].
Dalla-Man	10	Comprehensive model with brain, endogenous glucose and renal submodels [19, 40]. including counter-regulatory processes [39]

Finally, we review future challenge problems that will be useful in this space.

2 Related Work

The broader area of closed loop medical devices has received a lot of recent interest from the formal verification community. This started with work on pacemakers and implantable cardiac defibrillators (ICDs) that includes hybrid automata models for excitable cells in the heart [44], leading to approaches that employ these models to test closed loop systems [42, 31, 30]. We focus on reviewing the current state-of-the-art for verifying artificial pancreas controllers.

Human Insulin-Glucose Models: There have been many attempts to mathematically model how blood glucose levels respond to the infusion of insulin using ordinary differential equations (see Table 1). Examples include the well-known Bergman minimal model [3, 4], Dalla Man et al. model [38, 19, 39] and the Hovorka et al. model [28, 53]. These models incorporate features including the effect of meals, and more recently, the effects of exercise on the blood glucose levels [39]. In fact, the concept of *in silico* pre-clinical trials involves using these models to test control algorithms over "virtual subjects" by simulating a (virtual) clinical protocol [37, 43]. The simulation uses fixed meal timings, amounts and boluses, but varying patient parameter sets that are meant to model inter-patient variations. The simulations collect statistics on performance measures such as the time in euglycemic range to pre-judge the efficiency of the control algorithm and evaluate suggested changes. However, we note that the main objective of these trials is not to test the correctness of the closed loop per se. Beyond ODE-based models, there have been attempts at using delay differential equations (DDEs) (Cf. [35, 32] for instance) and fractional-order models [26].

Verification and Falsification Efforts: The broader area of hybrid systems verification has seen promising model checkers such as SpaceEx for affine hybrid systems [24] and tools such as

dReach, CORA, NLToolBox and Flow* for nonlinear hybrid systems [2, 51, 33, 13].

Chen et al. study a PID-based closed loop system meant for intraoperative use in patients. They use the dReal SMT solver [25] to find patient parameter ranges and ranges for controller gains for which a PID controller is proven to be safe with respect to specified safety properties [10]. The use of dReal SMT solver provides an exhaustive guarantee that all behaviors of the model are accounted for. The work of Chen et al. represents an important proof of concept that exhaustive safety verification required for proving the correctness of artificial pancreas control algorithms can, in principle, be performed by existing tools for nonlinear hybrid systems. However, major disturbances including patient meals and sensor noise that are common causes of algorithmic failures are not treated in their study.

Our past work in this space has focused on the problem of *falsification* rather than verification. Through falsification, we perform a best effort search focused on discovering behaviors of the closed loop system that violate a key property of interest specified using a real-time temporal logic. In the limit, falsification techniques either terminate with a counterexample to the property of interest or run for a long time without discovering any violations. In the latter case, it can output useful information such as the *least robust trace* but cannot conclude if the property is in fact valid for the system under test. Recent work on falsification uses the notion of temporal logic robustness [23, 21] to provide a real-valued distance to satisfaction or violation for a signal with respect to a property expressed in MTL/STL. This has been incorporated in tools such as S-Taliro [41, 1] and Breach [20] that search for falsifying traces through minimizing robustness of the trace. Even though falsification uses a simulation model such as the Dalla Man model, the final result is a *property violation* rather than a proof.

In joint work with Cameron and others, we have studied the use of falsification techniques for verifying closed loop control systems for the artificial pancreas [8]. Our initial work investigated a PID controller proposed by Steil et al. [52, 50, 49] based on published descriptions of the control system available. The simulation environment incorporates this controller in a closed loop with models of the patient [40], the sensors and actuators. We studied nearly six different temporal properties of the closed loop and obtained falsification for three of them. However, we could not falsify the remaining three properties that governed the absence of prolonged hypoglycemia and hyperglycemia in the patient.

Another recent study [45] was performed to test a predictive pump shutoff controller designed by Cameron et al. [7] that has undergone outpatient clinical trials, recently [36]. This study involved the entire controller software *as is*, without any modifications. At the same time, the closed loop simulation permits us to pose a rich set of questions that compare the closed loop performance with a corresponding open loop under the same meal inputs and physiological model conditions. The falsification discovered adverse noise patterns in the CGM sensor that could trick the Kalman filter into predicting inaccurate forecasts for the future glucose value, and thus prevent appropriate pump shutoff/resumption. At the same time, critical properties such as not commanding excess insulin when the patient is in hypoglycemia could not be violated. The study concluded the need to investigate these violations under more realistic patterns of CGM noise.

In this paper, we study a simpler hybrid control system that switches between multiple basal levels based on ranges of blood glucose values reported by the sensor. The control system is very simple to model using automata. The focus of our work is to explore exhaustive verification in the presence of sensor noise and meal disturbances using a nonlinear model. We demonstrate modifications to the Flow* tool that enable us to successfully carry out this verification task within half an hour for each run of the Flow* tool.

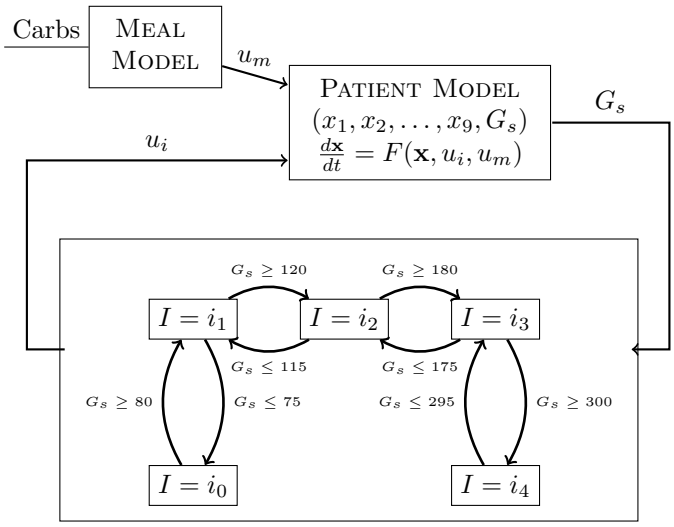

Figure 2: Overall closed loop controller setup for the artificial pancreas with patient and meal models and a multi-basal controller.

3 Model and Its Simplification

Figure 2 shows the overall block diagram of the model including the Dalla-Man model for insulin glucose regulation, a meal model for the gut absorption of ingested meals and the controller that manages the insulin infusion level as a function of the current glucose level.

3.1 Meal Absorption Model

We first examine the meal absorption model that models the glucose rate of appearance $u_m(t)$ corresponding to a meal with D grams of Carbohydrates (CHO) at time $t = t_m$. The original model is taken from Dalla man et al. [38] has three state variables $q_{\text{sto1}}, q_{\text{sto2}}, q_{\text{gut}}$ which model the amount of glucose in solid phase in the stomach, liquid phase in the stomach and the intestine, respectively. These are initialized to 0 at $t = 0$. Their dynamics are modeled as

$$\begin{aligned} \dot{q}_{\text{sto1}} &= -\mathsf{k}_{21} \cdot q_{\text{sto1}} + D \cdot \delta(t - t_m) \\ \dot{q}_{\text{sto2}} &= -\mathsf{k}_{\text{empt}}(q_{\text{sto1}} + q_{\text{sto2}}) \cdot q_{\text{sto2}} + \mathsf{k}_{\text{max}} \cdot q_{\text{sto1}} \\ \dot{q}_{\text{gut}} &= -\mathsf{k}_{\text{abs}} \cdot q_{\text{gut}} + k_{\text{empt}}(q_{\text{sto1}} + q_{\text{sto2}}) \cdot q_{\text{sto2}} \\ u_m(t) &= \mathsf{f} \cdot \mathsf{k}_{\text{abs}} \cdot q_{\text{gut}}(t) \end{aligned} \tag{1}$$

Here $k_{\text{empt}}(\cdot)$ is a nonlinear function given by

$$k_{\text{empt}}(q) = \mathsf{k}_{\text{min}} + \frac{1}{2} \cdot (\mathsf{k}_{\text{max}} - \mathsf{k}_{\text{min}}) \cdot \{\tanh(\alpha(q - \mathsf{b} \cdot D)) - \tanh(\beta(q - \mathsf{c} \cdot D)) + 2\}$$

Note that the impulse $\delta(t) = 1$ whenever $t = 0$ and 0 otherwise, modeling the ingestion of the meal as an instantaneous impulse. However, a more realistic meal is modeled as a square wave shaped function lasting for $t_d = 15$ minutes, with the carbohydrates ingested at a rate of $\frac{D}{15}$ grams/minute over this time period.

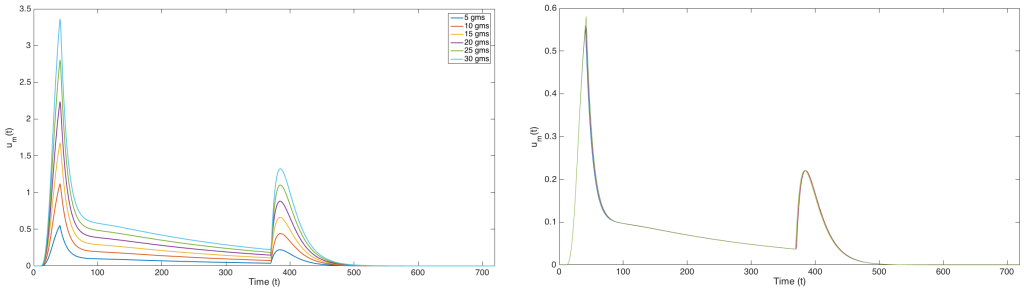

Figure 3: (**Left**) Meal model ODE in Eq. (1) simulated for different meal CHO amounts and (**Right**) simulations are scaled down by the amount of CHO to overlay on the simulation for $D = 5$ gms of CHO.

The values of the parameters $\mathsf{k}_{21}, \mathsf{k}_{\max}, \mathsf{k}_{\text{abs}}, \mathsf{k}_{\min}, \alpha, \beta, \mathsf{b}, \mathsf{c}$ are estimated by fitting to tracer labeled meal data collected from nearly 41 subjects [38, 19].

The presence of tanh function makes the model harder to work with inside a set-valued verification tool. Figure 3 shows the rate of appearance of glucose $u_m(t)$ as a function of time for meals with $D = 5, 10, \ldots, 30$ grams of CHO, ingested at $t_m = 10$ minutes. We simplify the model considerably by noting two properties of the model, empirically using the published parameter values.

1. Multiphase response to meals: we note that there are six easily identified qualitative phases in the meal absorption model and further more the switching time is *mostly* invariant to the meal composition.

2. Scaling property: the response for a meal with λD grams of CHO is *very close* to λ times that of a meal with D grams of CHO.

We exploit these properties and fit a piecewise quadratic function $u_{m,1}(t)$ so that we can simply obtain

$$u_m(t) = D u_{m,1}(t - t_m), \text{ for meal at time } t_m\,.$$

Here, the function $u_{m,1}(t)$ is fit using a regression model based on simulating the ODE in (1).

$$u_{m,1}(t) = \begin{cases} 0 & t \le 0 \\ 1.141 \times 10^{-4} t^2 + 6.134 \times 10^{-6} t & 0 \le t \le 30 \\ 5.25 \times 10^{-5} t^2 - 7.468 \times 10^{-3} t + 0.281 & 30 < t \le 80 \\ 1.245 \times 10^{-7} t^2 - 9.112 \times 10^{-5} t + 2.648 \times 10^{-2} & 80 < t \le 360 \\ -6.307 \times 10^{-5} t^2 + 0.0483 t - 9.190 & 360 < t \le 400 \\ 3.553 \times 10^{-6} t^2 - 3.423 \times 10^{-3} t + 0.824 & 400 < t \le 500 \\ 1.113 \times 10^{-8} t^2 - 1.482 \times 10^{-5} t + 4.9 \times 10^{-3} & 500 < t \le 720 \\ 0 & t \ge 720 \end{cases} \tag{2}$$

Note that we do not enforce the continuity of the various pieces of $u_m(t)$. Empirically, we note that the piecewise polynomial model in Eq. (2) approximates the model in ODE (1) within a tolerance of about $0.03D$ for a meal with D grams of CHO for $0 \le D \le 150$. At the same time, the quality of the fit, especially the undershoot can be improved further by adding

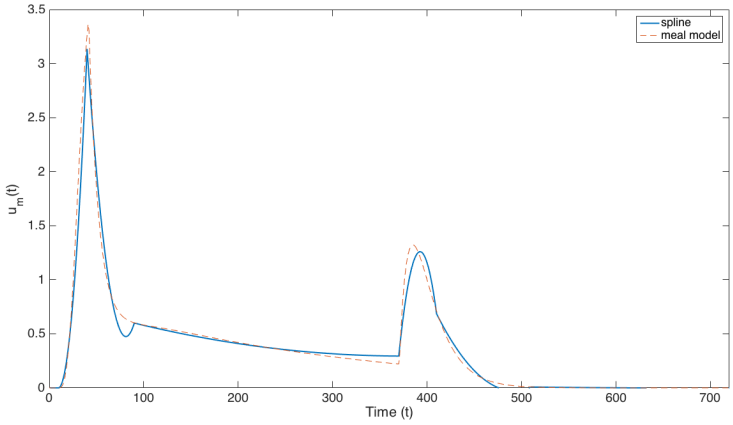

Figure 4: The piecewise polynomial (spline) approximation of the meal response Eq. (2) shown against the original meal response from ODE (1) (dashed line).

more constraints to the regression process for fitting the model. Nevertheless, the relatively tiny difference between the two models allows us to claim that the meal model model is a good approximation that can serve the purposes of the verification.

Formally reasoning about ODE (1) requires us to add a suitable interval to the model $u_m(t)$ from Eq. (2) and even prove a formal containment relation. We note however, that the original ODE model is itself an approximation to error prone lab measurements from tracer-labeled meal studies and intravenous glucose tolerance tests (IGTT). Since the ODE is but an approximation of this "ground truth", we will simply adopt the piecewise quadratic model as a more convenient approximation for our verification purposes.

3.2 Insulin-Glucose Response Model

We now turn to the insulin-glucose response model. Table 2 shows the state variables and the ODEs for this model [19]. The model captures many aspects of human insulin-glucose response including the insulin dependent vs. independent uptake of glucose, the endogenous production of glucose by the liver, the transport of subcutaneously administered insulin and subcutaneous glucose levels. It does not capture the counter-regulatory system including the effects of glucagon, prolonged fasting and physical activity. Nevertheless, the model has been approved by the FDA as a replacement for animal trials. The model depends intimately on using "virtual patient parameters": a set of such parameters corresponding to adult, adolescent and children are available with the commercial UVa-Padova T1D simulation software. The

Table 2: The state variables in the Dalla-Man model for the human insulin glucose response in people with type-1 diabetes.

Var.	Meaning
X	Insulin Conc. in remote chamber
I_{sc1}	Subcutaneous insulin in chamber #1
I_{sc2}	Subcutaneous insulin in chamber #2
G_t	Glucose conc. in "rapidly equilibriating" tissues
G_p	Glucose conc. in plasma
I_l	Portal vein insulin concentration
I_p	Insulin in plasma
I_1	Insulin chamber # 1 concentration
I_d	"delayed" insulin from chamber #1
G_s	subcutaneous glucose concentration.

state variables are shown in Tab. 2. The ODE uses a publicly available parameter set [19].

$$
\begin{aligned}
\dot{X} &= -0.0278X + 0.0278(18.2129I_p - 100.25) \\
\dot{I}_{\text{sc1}} &= 0.0142I_{\text{sc1}} - 0.0078I_{\text{sc2}} + u_I(t) \\
\dot{I}_{\text{sc2}} &= 0.0152I_{\text{sc1}} - 0.0078I_{\text{sc2}} \\
\dot{G}_t &= -0.0039(3.2267 + 0.0313X)G_t(1 - 0.0026G_t + 2.5097 \times 10^{-6}G_t^2) \\
&\quad +0.0581G_p - 0.0871G_t \\
\dot{G}_p &= 3.7314 - 0.0047G_p - 0.0121I_d - 0.0581G_p + 0.0871G_t + u_m(t) \\
\dot{I}_l &= -0.4219I_l + 0.225I_p \\
\dot{I}_p &= -0.315I_p + 0.1545I_l + 1.9 \times 10^{-3}I_{\text{sc1}} + 7.8 \times 10^{-3}I_{\text{sc2}} \\
\dot{I}_1 &= -0.0046(I_1 - 18.2129I_p) \\
\dot{I}_d &= -0.0046(I_d - I_1) \\
\dot{G}_s &= 0.1(0.5521G_p - G_s)
\end{aligned}
$$

Control Algorithm: We consider a simple multi-basal control algorithm based on the *control-to-range* paradigm that seeks to adjust the insulin rate to treat extreme fluctuations of the blood glucose levels by switching to progressively higher insulin rates to treat high BG values and suspending insulin delivery to treat lows. The template for the controller is shown in Figure 2, wherein the controller switches between discrete insulin delivery rates depending on the currently sensed glucose value. These levels can be tuned for a particular patient by carefully examining their recent insulin pump and continuous glucose monitor (CGM) data. The controller proposed here is a simple automaton-based system *proposed as a benchmark for verification* rather than a *proposed design for clinical use*. The complete algorithm needs to handle user inputs such as meal boluses or correction factors that the user may command, for instance by falling back to a fixed basal rate whenever the user commands a manual injection. Exercise based shutoff is another feature not considered here. The verification of a full-fledged system with these features will be part of our future work. However, recent open source systems such as the OpenAP share some of the features such as setting a higher or lower basal insulin delivery rate based on multiple factors that include the current insulin on board in addition to the blood glucose levels [18].

Clinical Simulation Scenario: We will assume the following scenario for our in-silico verification setup:

1. Patient ingests a meal with $D \in [50, 90]$ grams of CHO at time $t = 0$.
2. The patient's initial blood glucose levels can be anywhere in the range $[120, 160]$ mg/dl at time $t = 0$.
3. The controller is switched on at that time and runs for 720 minutes (12 hours) overnight, during which time the patient does not ingest any further meals.
4. The continuous glucose monitor (CGM) is subject to a noise that can be ± 10 mg/dl away from the actual value predicted by the model.

We note that the noise model assumes that any possible noise signal within the range is allowed. This is much more conservative than the CGM errors that are temporally correlated with each other [22]. On the other hand, miscalibration or faults can often lead to errors much larger in magnitude than ± 10 mg/dl. However, we note that no algorithm can be expected perform well under large errors, since the algorithm cannot, in general, distinguish a faulty sensor reading from an accurate value. As a result, we seek to verify the closed loop under "reasonable" error conditions.

Correctness Properties: We will consider important correctness properties for our work:

- The blood glucose levels should never fall below 70 mg/dl. Levels below 70 mg/dl are called *hypoglycemia*, and may lead to loss of consciousness or coma.
- The blood glucose levels should never rise above 300 mg/dl. Levels above 300 mg/dl expose the patient to a dangerous condition called ketoacidosis.
- The blood glucose should be in the *euglycemic* range $[70, 180]$ mg/dl during "wakeup" $t \in [600, 720]$.

4 Reachability Analysis

We introduce the algorithm to compute Taylor model flowpipes which are reachable set overapproximations for the artificial pancreas model shown in Figure 2.

We call a set which consists of all reals between two rational bounds a, b such that $a \leq b$ an *interval*, and denote it by $[a, b]$. A *Taylor Model (TM)* is denoted by a pair (p, I), such that p is a degree-bounded polynomial over a set of variables $x_1, \ldots, x_2$, collectively denoted by $\vec{x}$, each of which ranges in an interval domain, and I is an interval [5]. A continuous function $f(\vec{x})$ is overapproximated by a TM $(p(\vec{x}), [a, b])$ over a domain D, if for all $\vec{x}_0 \in D$ we have that $p(\vec{x}_0) + a \leq f(\vec{x}_0) \leq p(\vec{x}_0) + b$. TMs can also be organized as vectors to provide overapproximations for vector-valued functions.

Given an ODE $\dot{\vec{x}} = f(\vec{x})$ with an initial condition $\vec{x}(0) \in X_0$, the exact solution is denoted by a *flowmap* φ_f such that $\vec{x}(t) = \varphi_f(\vec{x}_0, t)$. In general, φ_f cannot be obtained in a closed form. However, it can be tightly overapproximated by a TM $(p(\vec{x}_0, t), I)$ of some order $k > 0$ over a small time step $[0, \delta]$. Then the range of $(p(\vec{x}_0, t), I)$ with $\vec{x}_0 \in X_0$ and $t \in [0, \delta]$ forms an overapproximation of the *reachable set*, i.e., all ODE solutions, in that time step. Such a TM is also called a *flowpipe*. The technique to consecutively compute TM flowpipes is called

TM integration (see [6]). That is, each TM flowpipe $(p(\vec{x}_0, t), I)$ is an overapproximation of the flowmap $\vec{x}(t) = \varphi_f(\vec{x}_0, t_0 + t)$ with $\vec{x}_0 \in X_0$, $t \in [0, \delta]$ for some $t_0 \geq 0$ which is the total amount of time covered by the previous flowpipes.

The main algorithm to compute TM flowpipes for the artificial pancreas model is an adaption of the general flowpipe construction framework for hybrid systems [11]. We present it as Algorithm 1.

Algorithm 1 Flowpipe construction algorithm for the artificial pancreas model

Input: Initial set X_0 of the model, initial dynamics $\mathcal{D}_0$, control stepsize δ_c, number of control steps N.

Output: Overapproximation of the reachable set in N control steps.

$\mathcal{R} \leftarrow \emptyset$; # set for resulting flowpipes
Enqueue $\langle X_0, 0, \mathcal{D}_0 \rangle$ to Queue; # Queue for new flowpipes
while Queue is not empty **do**
  Dequeue a state set $\langle X, n, \mathcal{D} \rangle$ from Queue;
  Compute the flowpipes from X in the time interval $[0, \delta_c]$ under $\mathcal{D}$;
  Add the flowpipes to $\mathcal{R}$;
  Compute the flowpipe X_{δ_c} at the time δ_c;
  Decide the possible dynamics $\mathcal{D}_1, \ldots, \mathcal{D}_m$ for the next control step;
  if $n < N$ **then**
    for all $i = 1, \ldots, m$ **do**
      Reduce X_{δ_c} to X_i according to the condition of $\mathcal{D}_i$;
      Enqueue $\langle X_i, n + 1, \mathcal{D}_i \rangle$ to Queue; # Add a new flowpipe
    end for
  end if
end while
return $\mathcal{R}$;

In each iteration of the main loop, the algorithm computes all flowpipes in a control step and determine the dynamics for the next step based on the flowpipe at the end of the current step along with the control strategy. It terminates when the given maximum number of control steps are handled. The dynamics in each step is an ODE that is derived from the control strategy shown in Figure 2. More details are given as follows.

Computing flowpipes in a control step. The flowpipe construction in each control step can be handled by the TM integration method, since the ODE is fixed. We use the efficient integrator with adaptive time steps implemented in Flow* [13]. Then, the flowpipe at the end of the control step can be easily evaluated from the last flowpipe.

Deciding the dynamics for the next control step. Since the discrete controller interferes the system only at the end of each control step, we only need to update the dynamics at the end of a step. For the strategy presented in Figure 2, our algorithm first evaluates the range of the glucose level G from the flowpipe X_{δ_c}, and then check the possibility of the insulin rates for the next step. It could be possible that the range of G covers the conditions for several insulin rates. If so, we subdivide the flowpipe X_{δ_c} according to those conditions and add each subdivision with the new dynamics into the queue. There are various methods to subdivide a TM flowpipe, we do it in the following way. Given a flowpipe X_{δ_c} whose range satisfies

the conditions $C_1, \ldots, C_m$, then the subdivision X_i for the condition C_i can be obtained from reducing X_{δ_c} according to C_i by domain contraction [12].

Theorem 1. *Algorithm 1 returns an overapproximation of the reachable set of the artificial pancreas model in N control steps.*

Although time triggered jumps can be modeled in a hybrid automaton by adding an extra timer variable, we need to intersect the flowpipes at the end of each control step using a standard event triggered semantics. The method not only is less efficient but also produces flowpipes which are unnecessarily large. The idea in Algorithm 1 is to perform a flowpipe construction for a control step and simply evaluate the TM overapproximation for the reachable set at the end of the step, it avoids an intersection computation which is required in the standard reachability computation framework.

We now consider the problem of incorporating a sensor error in the range $[-\Delta, \Delta]$ for each controller execution.

Sensor Noise. For a glucose value G_0, the effect of sensor noise results in a new value $G_0' \in [G_0 - \Delta, G_0 + \Delta]$. Given that the range of the glucose value is overapproximated by a TM X_G at the beginning of a control step, then a dynamics $\mathcal{D}$ is possible in the next step if its condition C is satisfied by a glucose value $G_0' \in \{G_0 + u \,|\, G_0 \in X_G, u \in [-\Delta, \Delta]\}$. If so, we may further reduce the TM X_G properly according to C and add it along with $\mathcal{D}$ to the queue. More precisely, if C is given by $G \leq a$, we may reduce X_G according to the constraint $G \leq a + \Delta$, since any value larger than $a + \Delta$ will not be deviated to a value below a by the noise. The case of $G \geq a$ can be treated analogously.

Merging flowpipes. Subdivisions on flowpipes may lead to an explosion of the sets in the queue. Therefore, we consider to merge flowpipes during the flowpipe construction. When we enqueue a new flowpipe, we try to merge it with an existing flowpipe in the queue. We say that two flowpipes are mergeable if they are the reachable set overapproximations at the same time instance. In our work, we simply compute the merged flowpipe as an interval enclosure for the mergeable flowpipes. Furthermore, since Algorithm 1 is performing a BFS exploration. Therefore, the computation of reachable states at the $(j+1)^{th}$ time step proceeds only after performing all possible flowpipe merges at step j.

The effectiveness of our algorithms will be evaluated based on the experiments given in the next section.

5 Experiments

We implemented the flowpipe construction algorithm for the artificial pancreas model from Figure 2, by combining the piecewise quadratic meal model, the ODE insulin glucose regulation model with the controller. Our model implements the clinical scenario described in Section 3. The implementation is performed using an C++ API provided by the Flow* tool. The API will be documented and made available to developers in the near future. For the model checking, we consider the time horizon of 720 minutes and a control step size 5 minutes, so there are totally 144 control steps along each computation path. In all tests, we use an adaptive step size bounded by 0.2, a TM order of 3, cutoff threshold 10^{-8}, and remainder estimation $[-0.01, 0.01]$.

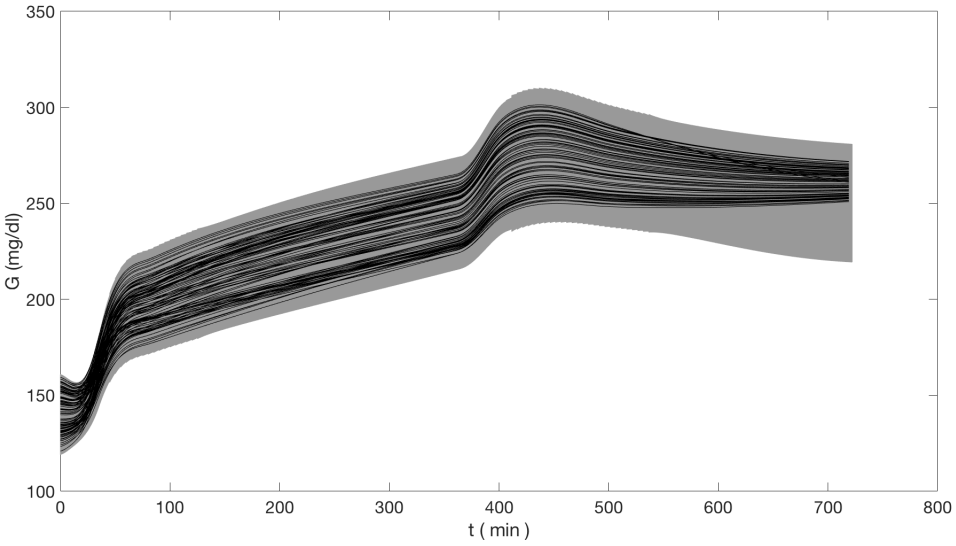

Figure 5: Flowpipes and numerical simulations without sensor noise (Strategy I)

We consider two different control strategies defined by sets of insulin rates. Control strategy I uses the insulin rates (see figure 2):

$$i_0 = 0.0,\ i_1 = 0.1,\ i_2 = 0.2,\ i_3 = 0.5,\ i_4 = 1.4\,.$$

Figure 5 shows the flowpipes computed by our algorithm without any sensor noise. The computation time required is 239 seconds. Figure 6 shows the flowpipes that take a sensor noise with $\Delta = 10$ into account. The computation time required is 264 seconds.

It is easily seen from the flowpipes that (a) hypoglycemia can never happen under this clinical scenario since $G \geq 70$ mg/dl holds in all situations, (b) the flowpipes indicate the possibility of $G \geq 300$ although simulations do not confirm a violation, and (c) the wakeup blood glucose levels are not inside the euglycemia range of $[70, 180]$ mg/dl.

Next, we consider strategy II using the insulin rates

$$i_0 = 0.0,\ i_1 = 0.3,\ i_2 = 0.7,\ i_3 = 1.2,\ i_4 = 1.5\,.$$

The computed flowpipes without sensor noise are shown in Figure 7. The time cost is 316 seconds. When a sensor noise of $\Delta = 10$ is added, we have the flowpipes shown in Figure 8, the time cost is 223 seconds.

We conclude that using insulin rates given by strategy II, the overall control is improved since $G \geq 70$ mg/dl and $G \leq 300$ mg/dl both hold. Nevertheless, the property of wakeup euglycemia remains violated.

Challenge Problems: We conclude by observing that even though Flow* tool can be used to systematically verify nonlinear mathematical models of insulin glucose response, the overall challenge of systematically synthesizing control parameters $i_0, \ldots, i_4$ to find values that can

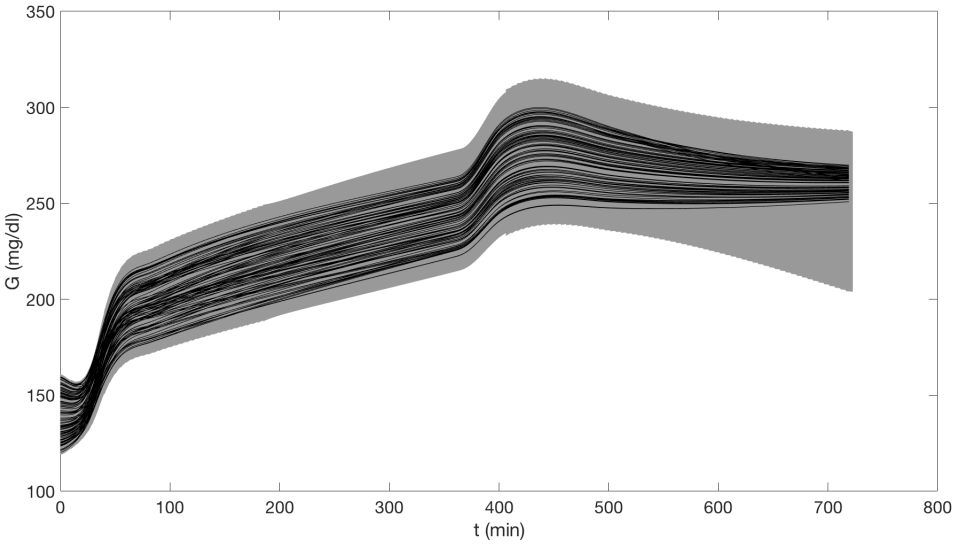

Figure 6: Flowpipes and numerical simulations with a sensor noise (Strategy I)

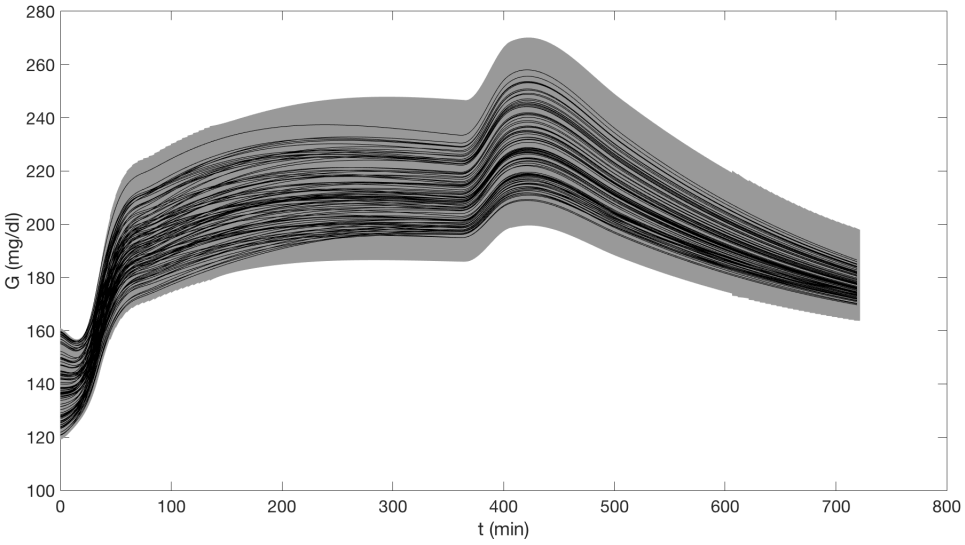

Figure 7: Flowpipes and numerical simulations without sensor noise (Strategy II)

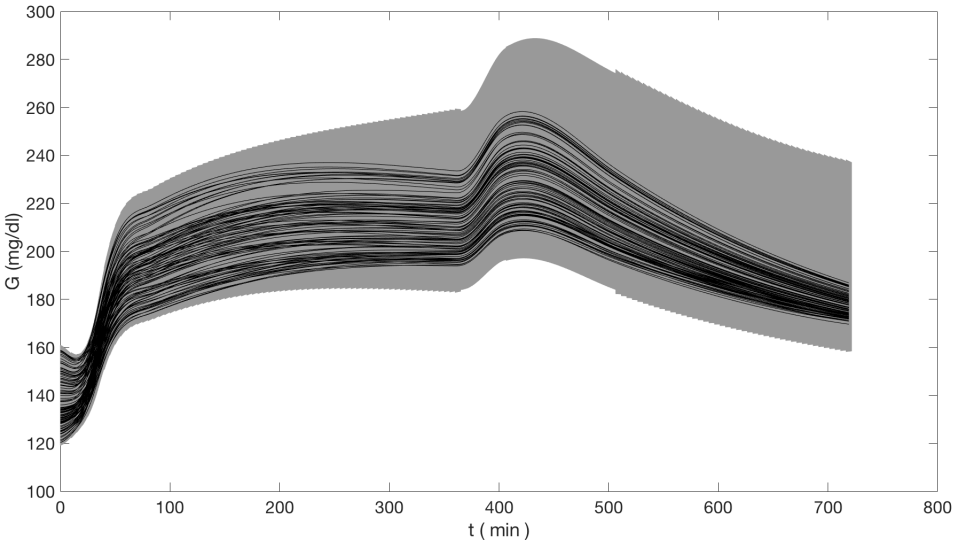

Figure 8: Flowpipes and numerical simulations with a sensor noise (Strategy II)

satisfy all three properties remains an open challenge for future verification efforts. Additionally, we may also consider a rich set of temporal correctness properties and richer clinical scenarios involving multiple meals. Finally, extending our approaches to the recently proposed extensions of the Dalla-Man model to incorporate the effect of physical activity remains part of our future work [39].

6 Conclusion

We present a model of artificial pancreas with a multi-basal controller. We propose a new flowpipe construction algorithm to compute reachable set overapproximations for the controlled system. Although such a system has 10 continuous variables and involves a large number of control switches, our method can still prove the safety for a challenging control strategy. In the future, we plan to study more complex control strategies using relational abstraction [46] and decomposition [14].

Acknowledgments: The authors gratefully acknowledge the anonymous reviewers for their useful comments and suggestions. This work was supported by the US National Science Foundation (NSF) under award number CNS 1446900. All opinions expressed are those of the authors and not necessarily of NSF.

References

[1] Houssam Abbas, Georgios Fainekos, Sriram Sankaranarayanan, Franjo Ivancic, and Aarti Gupta. Probabilistic temporal logic falsification of cyber-physical systems. *Trans. on Embedded Computing*

Systems (TECS), 12:95–, 2013.

[2] M. Althoff. An introduction to cora 2015. In *Proc. of ARCH'15*, volume 34 of *EPiC Series in Computer Science*, pages 120–151. EasyChair, 2015.

[3] R. N. Bergman and J. Urquhart. The pilot gland approach to the study of insulin secretory dynamics. *Recent Progress in Hormone Research*, 27:583–605, 1971.

[4] Richard N. Bergman. Minimal model: Perspective from 2005. *Hormone Research*, pages 8–15, 2005.

[5] M. Berz. *Modern Map Methods in Particle Beam Physics*, volume 108 of *Advances in Imaging and Electron Physics*. Academic Press, 1999.

[6] M. Berz and K. Makino. Verified integration of ODEs and flows using differential algebraic methods on high-order Taylor models. *Reliable Computing*, 4:361–369, 1998.

[7] F. Cameron, Darrell M. Wilson, Bruce A. Buckingham, Hasmik Arzumanyan, Paula Clinton, H. Peter Chase, John Lum, David M. Maahs, Peter M. Calhoun, and B. Wayne Bequette. Inpatient studies of a kalman-filter-based predictive pump shutoff algorithm. *J. Diabetes Science and Technology*, 6(5):1142–1147, 2012.

[8] Faye Cameron, Georgios Fainekos, David M. Maahs, and Sriram Sankaranarayanan. Towards a verified artificial pancreas: Challenges and solutions for runtime verification. In *Proceedings of Runtime Verification (RV'15)*, volume 9333 of *Lecture Notes in Computer Science*, pages 3–17, 2015.

[9] H. Peter Chase and David Maahs. *Understanding Diabetes (Pink Panther Book)*. Children's Diabetes Foundation, 12 edition, 2011. Available online through CU Denver Barbara Davis Center for Diabetes.

[10] Sanjian Chen, Matthew O'Kelly, James Weimer, Oleg Sokolsky, and Insup Lee. An intraoperative glucose control benchmark for formal verification. In 5^{th} *IFAC conference on Analysis and Design of Hybrid Systems (ADHS)*, Oct 2015.

[11] X. Chen. *Reachability Analysis of Non-Linear Hybrid Systems Using Taylor Models*. PhD thesis, RWTH Aachen University, 2015.

[12] X. Chen, E. Ábrahám, and S. Sankaranarayanan. Taylor model flowpipe construction for non-linear hybrid systems. In *Proc. of RTSS'12*, pages 183–192. IEEE Computer Society, 2012.

[13] X. Chen, E. Ábrahám, and S. Sankaranarayanan. Flow*: An analyzer for non-linear hybrid systems. In *Proc. of CAV'13*, volume 8044 of *LNCS*, pages 258–263. Springer, 2013.

[14] X. Chen and S. Sankaranarayanan. Decomposed reachability analysis for nonlinear systems. In *Proc. of the 37th IEEE Real-Time Systems Symposium (RTSS'16)*, pages 13–24. IEEE Computer Society, 2016.

[15] C. Cobelli, G. Federspil, G. Pacini, A. Salvan, and C. Scandellari. An integrated mathematical model of the dynamics of blood glucose and its hormonal control. *Mathematical Biosciences*, 58:27 – 60, 1982.

[16] Claudio Cobelli, Chiara Dalla Man, Giovanni Sparacino, Lalo Magni, Giuseppe De Nicolao, and Boris P. Kovatchev. Diabetes: Models, signals and control (methodological review). *IEEE reviews in biomedical engineering*, 2:54–95, 2009.

[17] Claudio Cobelli and Andrea Mari. Control of diabetes with artificial systems for insulin delivery — algorithm independent limitations revealed by a modeling study. *IEEE Trans. on Biomed. Engg.*, BME-32(10), Oct. 1985.

[18] # OpenAPS Community. Open artificial pancreas reference implementation. Cf. https://openaps.org/reference-design/.

[19] Chiara Dalla Man, Robert A Rizza, and Claudio Cobelli. Meal simulation model of the glucose-insulin system. *IEEE Transactions on Biomedical Engineering*, 1(10):1740–1749, 2006.

[20] Alexandre Donzé. Breach: A toolbox for verification and parameter synthesis of hybrid systems. In *CAV*, volume 6174 of *Lecture Notes in Computer Science*. Springer, 2010.

[21] Alexandre Donzé and Oded Maler. Robust satisfaction of temporal logic over real-valued signals. In *FORMATS*, volume 6246 of *Lecture Notes in Computer Science*, pages 92–106. Springer, 2010.

[22] Andrea Facchinetti, Giovanni Sparacino, and Claudio Cobelli. Modeling the error of continuous glucose monitoring sensor data: Critical aspects discussed through simulation studies. *J. Diabetes Sci. and Tech.*, 4(1), January 2010.

[23] Georgios Fainekos and George J. Pappas. Robustness of temporal logic specifications for continuous-time signals. *Theoretical Computer Science*, 410:4262–4291, 2009.

[24] G. Frehse, C. Le Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler. Spaceex: Scalable verification of hybrid systems. In *Proc. of CAV'11*, volume 6806 of *LNCS*, pages 379–395. Springer, 2011.

[25] Sicun Gao, Sonhoo Kong, and Edmund M. Clarke. dReal: an SMT solver for nonlinear theories over the reals. In *Proc. CADE'13*, volume 7898 of *Lecture Notes in Computer Science*, pages 208–214. Springer, 2013.

[26] M. Ghorbani and P. Bogdan. Reducing risk of closed loop control of blood glucose in artificial pancreas using fractional calculus. In *36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS)*, pages 4839–4842, Aug 2014.

[27] R. Hovorka, V. Canonico, L.J. Chassin, U. Haueter, M. Massi-Benedetti, M.O. Frederici, T.R. Pieber, H.C. Shaller, L. Schaupp, T. Vering, and M.E. Wilinska. Nonlinear model predictive control of glucose concentration in subjects with type 1 diabetes. *Physiological Measurement*, 25:905–920, 2004.

[28] R. Hovorka, F. Shojaee-Moradie, P.V. Carroll, L.J. Chassin, I.J. Gowrie, N.C. Jackson, R.S. Tudor, A.M. Umpleby, and R.H. Hones. Partitioning glucose distribution/transport, disposal and endogenous production during IVGTT. *Am. J. Physiol. Endocrinol. Metab.*, 282:992–1007, 2002.

[29] Roman Hovorka. Continuous glucose monitoring and closed-loop systems. *Diabetic Medicine*, 23(1):1–12, 2005.

[30] Zhihao Jiang, Miroslav Pajic, Rajeev Alur, and Rahul Mangharam. Closed-loop verification of medical devices with model abstraction and refinement. *International Journal on Software Tools for Technology Transfer*, pages 1–23, 2013.

[31] Zhihao Jiang, Miroslav Pajic, Salar Moarref, Rajeev Alur, and Rahul Mangharam. Modeling and verification of a dual chamber implantable pacemaker. In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, volume 7214 of *Lecture Notes in Computer Science*, pages 188–203. 2012.

[32] Stephen M. Kissler, Cody Cichowitz, Sriram Sankaranarayanan, and David M. Bortz. Determination of personalized diabetes treatment plans using a two-delay model. *J. Theor. Biol.*, (accepted), 2014.

[33] S. Kong, S. Gao, W. Chen, and E. M. Clarke. dreach: δ-reachability analysis for hybrid systems. In *Proc. of TACAS'15*, volume 9035 of *LNCS*, pages 200–205. Springer, 2015.

[34] Aaron Kowalski. Pathway to artificial pancreas revisited: Moving downstream. *Diabetes Care*, 38:1036–1043, June 2015.

[35] Jiaxu Li, Yang Kuang, and Clinton C. Mason. Modeling the glucose-insulin regulatory system and ultradian insulin secretory oscillations with two explicit time delays. *J. Theor. Biol.*, 242(3):722–35, October 2006.

[36] David M. Maahs, Peter Calhoun, Bruce A. Buckingham, and Others. A randomized trial of a home system to reduce nocturnal hypoglycemia in type 1 diabetes. *Diabetes Care*, 37(7):1885–1891, July 2014.

[37] L. Magni, D.M. Raimondo, L. Bossi, C. Dalla Man, G. De Nicolao, B. Kovatchev, and C. Cobelli. Model predictive control of type 1 diabetes: an *in silico* trial. *J. Diabetes Science and Technology*, 1(6):804–12, 2007.

[38] Chiara Dalla Man, Michael Camilleri, and Claudio Cobelli. A system model of oral glucose absorption: Validation on gold standard data. *Biomedical Engineering, IEEE Transactions on*,

53(12):2472 –2478, dec. 2006.

[39] Chiara Dalla Man, F. Micheletto, D. Lv, M. Breton, Boris Kovatchev, and Claudio Cobelli. The UVA/PADOVA type 1 diabetes simulator: New features. *J. Diabetes Science and Technology*, 8(1), January 2014.

[40] Chiara Dalla Man, Davide M. Raimondo, Robert A. Rizza, and Claudio Cobelli. GIM, simulation software of meal glucose-insulin model. *J. Diabetes Sci. and Tech.*, 1(3), May 2007.

[41] Truong Nghiem, Sriram Sankaranarayanan, Georgios E. Fainekos, Franjo Ivančić, Aarti Gupta, and George J. Pappas. Monte-carlo techniques for falsification of temporal properties of non-linear hybrid systems. In *Hybrid Systems: Computation and Control*, pages 211–220. ACM Press, 2010.

[42] M. Pajic, R. Mangharam, O. Sokolsky, D. Arney, J. Goldman, and I Lee. Model-driven safety analysis of closed-loop medical systems. *Industrial Informatics, IEEE Transactions on*, 10(1):3–16, Feb 2014.

[43] S.D. Patek, B.W. Bequette, M. Breton, B.A. Buckingham, E. Dassau, F.J. Doyle III, J. Lum, L. Magni, and H. Zisser. In silico preclinical trials: methodology and engineering guide to closed-loop control in type 1 diabetes mellitus. *J Diabetes Sci Technol.*, 3(2):269–82, 2009.

[44] Y. Pei, E. Entcheva, R. Grosu, and S.A. Smolka. Efficient modeling of excitable cells using hybrid automata. In *Proc. Computational Methods in Systems Biology*, pages 216–227, 2005.

[45] Sriram Sankaranarayanan, Suhas Akshar Kumar, Faye Cameron, B. Wayne Bequette, Georgios Fainekos, and David M. Maahs. Model-based falsification of an artificial pancreas control system. *ACM SIGBED Review (Special Issue on Medical Cyber Physical Systems)*, 2016. To Appear, Nov 2016.

[46] Sriram Sankaranarayanan and Ashish Tiwari. Relational abstractions for continuous and hybrid systems. In *CAV*, volume 6806 of *LNCS*, pages 686–702. Springer, 2011.

[47] Gary Scheiner. *Think like a pancreas: A Practical guide to managing diabetes with insulin.* Da Capo Press, 2011.

[48] J.T. Sorensen. *A Physiological Model of Glucos Metabolism in Man and its use to Design and Access Improved Insulin Therapies for Diabetes.* PhD thesis, Massachussetts Inst. of Technology (MIT), 1985.

[49] Garry M. Steil. Algorithms for a closed-loop artificial pancreas: The case for proportional-integral-derivative control. *J. Diabetes Sci. Technol.*, 7:1621–1631, November 2013.

[50] G.M. Steil, A.E. Panteleon, and K. Rebrin. Closed-sloop insulin delivery - the path to physiological glucose control. *Advanced Drug Delivery Reviews*, 56(2):125–144, 2004.

[51] R. Testylier and T. Dang. Nltoolbox: A library for reachability computation of nonlinear dynamical systems. In *Proc. of ATVA'13*, volume 8172 of *LNCS*, pages 469–473. Springer, 2013.

[52] S Weinzimer, G Steil, K Swan, J Dziura, N Kurtz, and W. Tamborlane. Fully automated closed-loop insulin delivery versus semiautomated hybrid control in pediatric patients with type 1 diabetes using an artificial pancreas. *Diabetes Care*, 31:934–939, 2008.

[53] M.E. Wilinska, L.J. Chassin, C. L. Acerini, J. M. Allen, D.B. Dunber, and R. Hovorka. Simulation environment to evaluate closed-loop insulin delivery systems in type 1 diabetes. *J. Diabetes Science and Technology*, 4, January 2010.