出力制約つき関数リアクティブシステムにおける入力センサの静的仕様推定

白鳥佑弥・森口草介・渡部卓雄 (東京工業大学)

概要

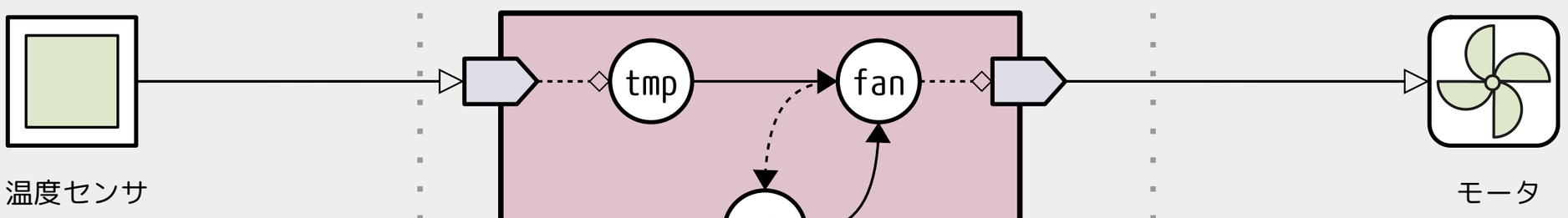
- 出力に繋がれたアクチュエータを故障させないために，関数リアクティブシステムの出力に制約を設ける
- 出力の制約を満たすために十分な入力センサの仕様を，SMTソルバであるZ3を用いて静的に推定する
- 推定を高速に行うために，システムのノード(時変値)の性質を利用して制約式を変形させる

問題設定

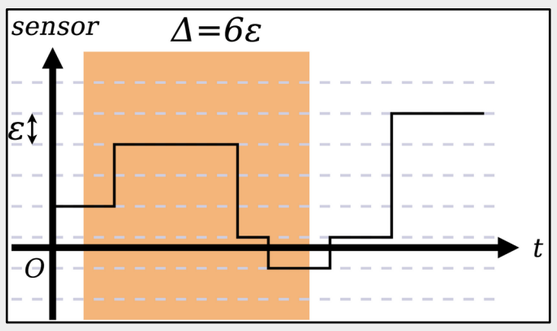
1つのセンサを入力とした関数リアクティブシステムを考える。このシステムの出力に関する N 個の条件式 $P_1, \cdots, P_N$ を順に満たす瞬間が観測されたとき，P_1 を満たしてから P_N を満たすまでに最短でも d 秒かかるという制約を**出力制約**と定め，Duration Calculus [Chaochen 1991] に基づく記法で

$$\Box(\lceil P_1 \rceil \rhd \cdots \rhd \lceil P_N \rceil \Rightarrow \ell \geq d)$$

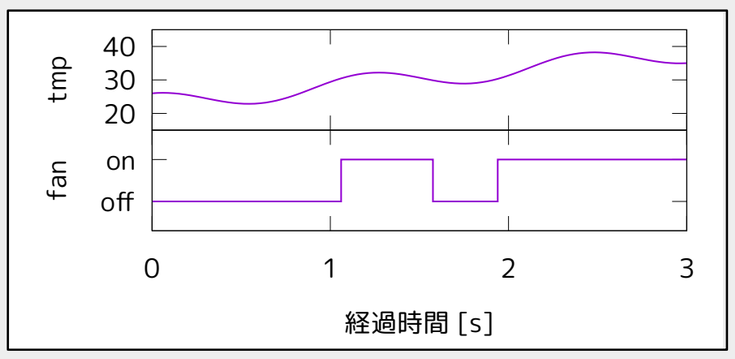
と表す。本研究では，システムが出力制約を満たすために十分なセンサの分解能 ε と1秒あたりの最大累計変化量 Δ_{max} の値を推定する。以下は問題の例である。



入力センサは単一の実数値を測定値とし，分解能 ε と，1秒後までに観測した変化の総和 Δ の最大値 Δ_{max} が固定であると仮定する。システム開始時の初期値は ε や Δ_{max} に依存せず任意の実数値をとり得るとする。



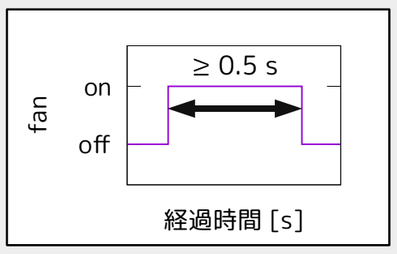

```
in tmp out fan

node init[False] fan: Bool = tmp >= th
node th: Real = 30.0 + (if fan@last then -1.0 else 1.0)
```



miniEmfrpで記述したコード例(上)と挙動の例(下)

モータの頻繁な起動停止は故障の原因となる。そこで，FanControllerシステムではモータがOFF, ON, OFFとなる瞬間を順に観測するとき，それは必ず 0.5 秒以上かかるという出力制約(♠)を考える。

$$\Box(\lceil \neg \mathrm{fan} \rceil \rhd \lceil \mathrm{fan} \rceil \rhd \lceil \neg \mathrm{fan} \rceil \Rightarrow \ell \geq 0.5) \cdots (♠)$$



提案手法

センサの分解能 ε の値が与えられているとき，出力制約を満たす Δ_{max} の値を次の手順で推定する。

1. 与えられたプログラムを制約式に変換し，出力制約を否定する制約式を作る
2. Z3が充足不能(unsat)を返す Δ_{max} の上限値を二分探索で求める
3. Δ_{max} の変化が ε/4 未満になったら探索を終了する

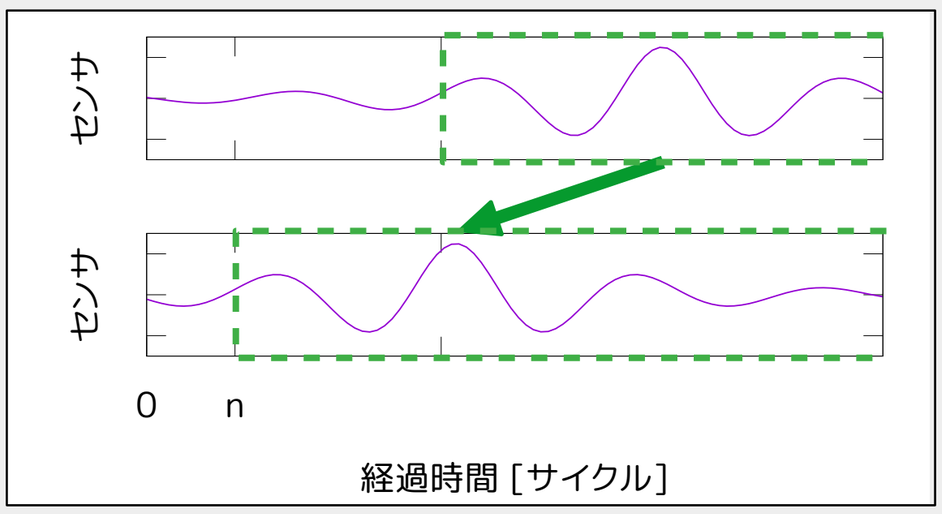
実験

FanController システムに出力制約 (♠) を与えたとき，各 ε に対して制約を満たす Δ_{max} の上限値を推定すると，下表のような結果が得られた。

ε [℃]	0.1	0.2	0.3	0.5	1.0
Δ_{max} の上限値 [℃]	2.2	2.4	2.4	3.0	4.0

再現可能性を利用した効率化

システムのある実行における時刻 n 以降の挙動を時刻 n からの挙動とするような別の実行が存在するというノードの**再現可能性**を調べることで，反例となる区間の探索を有限期間内に抑えられる(下図)。



今後の課題

- プログラムの構造に基づいた再現可能性の導出
- 入力が複数あるシステムにおけるセンサ仕様推定