ABS（アンチロック・ブレーキ・システム）を Event-B でモデル化する

株式会社ジェーエフピー

2011 年 10 月 27 日

本稿では ABS（アンチロック・ブレーキ・システム）を Event-B でモデル化する。まず、第 1 節で Event-B の概要と利点について説明する。実際のモデル化の様子は第 2 節で説明する。最後に、第 3 節では、これらの結果を踏まえて考察と提案を行う。

1　Event-B の特長

1.1　Event-B の概要

Event-B はシステムをモデル化し、そのモデルの正しさを論理学的に証明する手法である。Event-B は多数のソフトウェア開発プロジェクトで使われてきた。特に、安全性への要求が強い分野、例えば地下鉄の運行システムに採用例がある。

Event-B のモデルの中心となる概念は「状態」（state）と「遷移」（transition）である。Event-B はシステムの状態を、複数の変数（variable）とその値で表現する。一方、遷移は複数のイベントで表現する。それぞれのイベントは「ガード条件」（guard）と「動作」（action）で表現される。ガード条件とは、イベントが発生する条件を表す論理式である。また、動作は、システムの状態（具体的には、変数の値）を変化させる方法を定義するものである。

Event-B のモデルでは、ガード条件を満たすイベントのうちのいずれかが発生すると想定する。本稿の例では、イベントは 1 個だけであり、そのイベントは「時刻を単位時間だけ進める」ものである。このイベントには「自動車の速度が 0 より大きい」というガード条件が付いている。自動車の速度が 0 になると、他にイベントがないため、システムそのものが停止する。

Event-B のモデルを構成する他の要素には「定数」（constant）と「公理」（axiom）がある。定数は、いかなるイベントが発生しても変化することのないパラメータである。公理は、これらの定数が満たしている性質（properties）を示す論理式である。本稿では、公理には **axm** で始まるラベルを付けている。

Event-B のモデルにとって、さらに重要なのは「不変式」（invariant）である。これは、システムが満たすべき性質を論理式で表現したものである。「不変式」という呼び方は、イベントが発生してシステムの状態が変化しても、不変式は依然として成立していることから来ている。この不変式を証明することが、Event-B でモデルの正しさを証明することの中心になる。なお、不変式を証明する一般的な方法は、「イベント発生前に不変式が成立していたならば、イベント発生後にも不変式が成立している」ことを証明することである。本稿では、不変式には **inv** で始まるラベルを付けている。

最後に、イベントの「動作」の形式について説明を補足する。動作は決定的な（deterministic）定義と非決

定的な（non-deterministic）定義がある。決定的な定義では、イベント後の変数の値がただ一つに定まる。対照的に、非決定的な定義では、イベント後の変数の値は、可能な複数の値のうちのいずれかの値となる。決定的な定義は、たとえば以下のような形式である。

$$x := x + 1 \tag{1}$$

これは、変数 x の値を 1 増やすことを意味する。一方、非決定的な定義は以下のような形式である。

$$0 < x' \wedge x' \leq x \tag{2}$$

これは、変数 x のイベント後の値は、0 より大きく、イベント前の x の値よりは小さいことを意味する。プライムの付いた変数はイベント後、そうでない変数はイベント前を表し、これらの変数の関係を数式と論理式で表現する。

なお、Event-B の手法の特徴として、「精義化」（refinement）を挙げることができる。精義化とは、まず単純なモデルを作っておいて、それを少しずつ複雑化していくことである。最初から複雑なモデルを作ってしまうと、その性質を証明したり、間違いを修正したりするのがとても大変になる。まず単純なモデルを作り、そのモデルの正しさを証明しておいてから、次の段階に進むというのが Event-B の特徴である。

1.2 Event-B の利点

Event-B の利点として、システムの正しさを証明できることと、システムの理解が明確になることが挙げられる。まず、モデルを数式と論理式で記述することで、システムを客観的に理解することができる。さらに、システムの満たすべき性質を論理式で記述して、その論理式を証明することで、システムの「正しさ」を厳密に証明できる。

システムの設計を始める前に、Event-B によるモデル化と証明を行うことで、開発期間の短縮と、不具合の減少という効果が得られる。

1.3 力学的システムのモデル化

今回、取り上げる事例は、自動車の ABS（アンチロック・ブレーキ・システム）である。このシステムは物理法則に従って構築された力学的システムである。力学的システムの特徴として、時間と物理量が実数（連続量）で表されることが挙げられる。

これに対して、Event-B のモデルは離散時間である。そのため、時間の経過を「時刻を Δt だけ進める」というイベントで表現する。また、時間積分も離散時間に変換して記述する。

1.4 シミュレーションとの比較

Simulink などの製品を使うことで、数値計算によるシミュレーションが可能である。これを、Event-B のような、論理式による証明と比較すると、以下のような利点と欠点がある。

まず、論理式による証明では、考えられる全ての場合を網羅することができる。なぜなら、論理的に起こりうる全ての場合に対して、目的の論理式が成り立つことを証明するからである。その反面、特定の場合における具体的な結果を得ることができない。

これに対して、数値計算によるシミュレーションでは、具体的な値を入力したときの結果が得られる。その

ため、シミュレーションの結果を解釈することが容易であり、システムの動作を直観的に理解することができる。しかしながら、特定の入力に対する結果しか検証しないので、条件外の挙動を見落とす可能性がある。

2 実際のモデル

2.1 対象システム

本稿では ABS（アンチロック・ブレーキ・システム）をモデル化する。ABS とは、車両を停止させようとするとき、車輪の路面に対する滑りを抑制することで、制動距離を小さくするものである。ABS を持たない車両では、車輪と路面との間の滑りが大きくなると、摩擦係数が小さくなり、車両を減速する力が弱くなるという問題がある。ABS は、車輪と路面との滑りが大きい時には、自動的に、ブレーキ圧力をある程度まで低くする。すると、滑りが低減され、摩擦力が大きくなり、その結果、車両が早く停止するようになる。

ABS の仕様は Simulink のサンプル[*1]から取った。本稿では、同じ仕様を Eevnt-B でモデル化することを試みる。

2.2 仕様書の準備

作業の手順としては、まず、Simulink のサンプルをもとに、自然言語で仕様書を作成した。次に、この仕様書を「構造化仕様書[*2]」に整形した。構造化仕様書とは、仕様書を以下のように構造的に分類したものである。

1. 「要求」と「補足説明」を分離する。
2. 要求を自己完結した短い言明に区分けする。
3. それぞれの要求項目にラベルと番号を付ける。

さらに、構造化仕様書をもとに SLP 文書[*3]を作成した。これらの資料を通して、ABS の仕様の理解を明確にした上で、Event-B のモデルの作成に着手した。

構造化仕様書のそれぞれの要求項目には [FUN 1.2.3] のような形式のラベルと番号を付けた。この番号を SLP 文書と Event-B モデルにも記載することで、要求の対応付けを行った。本稿にも [FUN 1.2.3] のような形式の番号が記載されている。これは構造化仕様書の要求項目に対応する。

Event-B によるモデル作成と証明が終わったところで、モデル作成を通して得られた知見を、構造化仕様書と SLP 文書にフィードバックした。それにより追加された要求項目は、本稿では *[FUN 1.2.10]* のようなイタリック体で表記している。

2.3 精義化の戦略

ABS を Event-B でモデル化するにあたって、まず、精義化の戦略[*4]を定める。

Event-B では、まず全体像を俯瞰的にモデル化し、その後、精義化によって細部を詰めていく方法を取る。最初から複雑なモデルを作ってしまうと、その性質を証明したり、間違いを修正したりするのがとても大変だ

[*1] `http://www.mathworks.co.jp/products/simulink/demos.html?file=/products/demos/shipping/simulink/sldemo_absbrake.html`

[*2] 構造化仕様書は、Event-B の提唱者 Jean-Raymond Abrial の著書で採用されている、要求文書の形式である。

[*3] `http://www.jfp.co.jp/slp/`

[*4] Event-B ではモデルを作成する前に精義化の戦略を立てることを勧めている。

からである。本稿では、自動車の ABS をモデル化するにあたって、まずは自動車の走行と停止をモデル化した。このモデルには、ブレーキどころか車輪すら存在しない。それらは後の精義化で追加する。精義化をしていない最初のモデルは、できるだけシンプルに全体像を描出することが重要である。そのため、自動車全体の運動と力のみをモデル化した。

具体的な精義化のステップは以下のようになる。

まず、初期モデルでは、自動車の走行と停止をモデル化する。そのため、自動車の位置、速度、加速度を表す変数を定義する。また、自動車にかかる力を表す変数と、自動車の質量を表す定数を導入する。Event-B のモデルは離散時間なので、時刻を 1 単位だけ進めるイベントを定義して、自動車の物理現象をシミュレートする。

第 1 次精義化では、車輪を導入する。まず、車輪の半径を表す定数を用意する。続いて、車輪の角速度を導入する。また、自動車の速度と車輪の半径から得られる仮想的な角速度を「車両角速度」として定義する。最後に、車輪角速度と車両角速度からスリップ率を得る。

第 2 次精義化では、μ-スリップ曲線を導入する。μ-スリップ曲線は、スリップ率から摩擦率を得る関数である。私たちは、この曲線を折れ線で近似する。

第 3 次精義化では、車輪にかかる複数の力を導入する。ここでは、摩擦率から摩擦力とタイヤトルクを得る。また、ブレーキトルクを非決定的に導入する。

第 4 次精義化では、ブレーキ系を導入する。まず、制御系からブレーキ系への信号を非決定的に定義する。これをもとにブレーキ圧力とブレーキトルクを計算する。

第 5 次精義化では、バンバン制御を導入する。スリップ率と、その目標値から、ON/OFF 率を計算し、それをブレーキ系に送る。

最後に、これは精義化ではないが、2 台の自動車を比較する。第 4 次精義化で得られたモデルを精義化し、ブレーキ圧が常に増加し続けるモデルを作る。これは、ABS を持たない自動車をモデル化したものである。この「古典的な」自動車のモデルと、第 5 次精義化のモデルを比較して、可能ならば、後者の方が制動距離が常に小さくなることを証明する。

2.4 初期モデル：自動車の移動

初期モデルは、自動車が減速して停止するだけのモデルである（図 1）。自動車に後ろ向きにかかる力を F、自動車の質量を m とすると、自動車の減速度 d は $d = \frac{F}{m}$ [FUN 2.3.1] である。

自動車の初速を V_0 [FUN 2.3.2]、現在の時刻を t とすると、自動車の速度 V は $V_0 - \int_0^t d(t)dt$ [FUN 2.3.3] である。ここで、時間積分を離散システムとして近似する。現在の自動車の速度を V'、前時刻の自動車の速度を V、現在の減速度を d'、前時刻から現在の時刻までの時間を Δt とすると、$V' = V - d'\Delta t$ である。ただし、自動車の速度が負になる場合には、上記の式を適用せず、$V' = 0$ とする *[FUN 2.3.3a]*。

自動車の速度が 0 になったら、このシステムは停止する [FUN 3.1]。すなわち、全てのイベントが発生しなくなる。そうでなければ、「時刻を Δt 進める」イベントが発生する。このことから、現在の時刻を t'、前時刻を t とすると、$t' = t + \Delta t$ *[FUN 5.4]* である。また、時刻 t の初期値は 0 *[FUN 5.2]* とする。

また、自動車が進行した距離を x とする。これは時間積分により $x = \int_0^t V(t)dt$ [FUN 4.2] として求められる。これを離散化すると $x' = x + V'\Delta t$ となる。

以上の条件を Event-B の形式でモデル化する。まず $m, V_0, \Delta t, F_0$ を定数とする。なお、F_0 は力 F の初期値である。

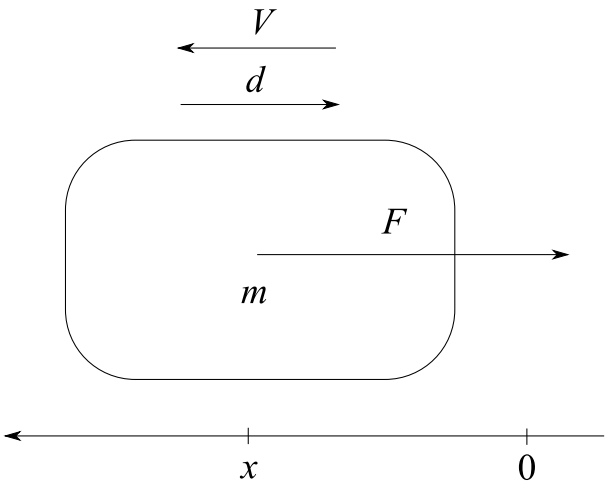

図 1　初期モデル

定数: m — **axm0_1**: $0 < m$ *[ENV 2.3.1]*
定数: V_0 — **axm0_2**: $0 < V_0$ *[ENV 2.3.2]*
定数: Δt — **axm0_3**: $0 < \Delta t$ *[FUN 5.1]*
定数: F_0 — **axm0_4**: $0 \leq F_0$ *[FUN 2.2.4]*

続いて F, d, t, V, x を変数とする。

変数: F — **inv0_1**: $0 \leq F$ *[FUN 2.2.5]*
変数: d — **inv0_2**: $0 \leq d$ *[FUN 2.3.7]*
変数: t — **inv0_3**: $d = \frac{F}{m}$ [FUN 2.3.1]
変数: V — **inv0_4**: $0 \leq t$ *[FUN 5.3]*
変数: x — **inv0_5**: $0 \leq V$ [FUN 3.1]
inv0_6: $0 \leq x$ *[FUN 4.4]*

減速度 d は力 F と質量 m から計算できるので、これらの関係を **inv0_3** に示している。速度 V は初速度 V_0 と減速度 d から計算できるが、時間積分が必要となるので、それぞれの時点で成立する不変式として表現することはできない。距離 x についても同様である。

初期イベント init は以下のようになる。

init
  $F := F_0$
  $d := \frac{F_0}{m}$ [FUN 2.3.1]
  $t := 0$ *[FUN 5.2]*
  $V := V_0$ [FUN 2.3.2]
  $x := 0$ [FUN 4.1]

時刻を Δt だけ進めるイベントは以下のようになる。

step
when

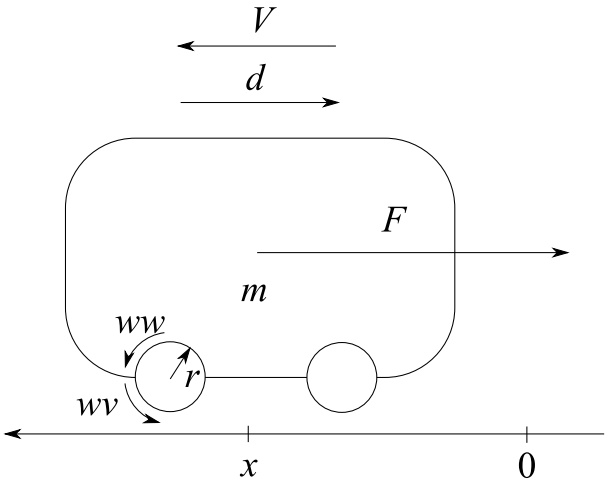

図 2　第 1 次精義化

$0 < V$ [FUN 3.1]
then
$0 \leq F'$ *[FUN 2.2.5]*
$d' = \frac{F'}{m}$ [FUN 2.3.1]
$t := t + \Delta t$ *[FUN 5.4]*
$0 \leq V - d'\Delta t \Rightarrow V' = V - d'\Delta t$ [FUN 2.3.3]
$V - d'\Delta t < 0 \Rightarrow V' = 0$ [FUN 2.3.3]
$x' = x + V'\Delta t$ [FUN 4.2]
end

力 F は予測不可能であると仮定して、前後述語 $0 \leq F'$ で非決定的に表現している。そのため、他の変数も非決定的に表現される。変数 t のみは、自分自身と定数 Δt から計算できるため、決定的に表現できる。

2.5　第 1 次精義化：車輪の導入

この精義化ではモデルに車輪を導入する（図 2）。まず車輪の半径を定数 r とする。変数は、車輪角速度 ω_w と車両角速度 ω_v を導入する。車両角速度は、車両の速度と車輪半径から求められる仮想的な角速度である。そのため、不変式 $\omega_v = \frac{V}{r}$ [FUN 2.3.4] を追加する。

車輪角速度と車両角速度を導入したので、スリップ率 *slip* も定義できる。これは $slip = 1 - \frac{\omega_w}{\omega_v}$ [FUN 2.1] で計算する。ただし、Rodin は数値は整数しか扱えないという制約がある。そのため、定数 S を用いてスリップ率を拡大する。すなわち、スリップ率は $slip = S - \frac{S\omega_w}{\omega_v}$ とする。なお、車輪角速度 ω_w と車両角速度 ω_v は前時刻の値を使用する [FUN 2.1] ので、式 $slip = S - \frac{S\omega_w}{\omega_v}$ を不変式として利用することはできない。かわりに、決定的な動作 $slip := S - \frac{S\omega_w}{\omega_v}$ をイベント step に記述する。

その他、初期モデルで使用した定数と変数はそのまま使用する。

定数: r　　**axm1_1**: $0 < r$ *[ENV 2.2.1]*
定数: S　　**axm1_2**: $0 < S$

スリップ率は 0 以上 1 以下 *[FUN 2.2, FUN2.3]*（私たちのモデルでは $0 \leq slip \leq S$）なので、$\omega_w \leq \omega_v$ *[FUN 2.3.8]* である。これを **inv1_2** に示す。

変数: ω_w
変数: ω_v
変数: *slip*

inv1_1: $0 \leq \omega_w$ *[FUN 2.4.6]*
inv1_2: $\omega_w \leq \omega_v$ *[FUN 2.3.8]*
inv1_3: $\omega_v = \frac{V}{r}$ [FUN 2.3.4]
inv1_4: $0 \leq slip$ *[FUN 2.2]*
inv1_5: $slip \leq S$ *[FUN 2.3]*

初期状態では $\omega_w = \omega_v$ である。ω_v は $\omega_v = \frac{V_0}{r}$ で初期化できる [FUN 2.3.5] ので、ω_w も全く同じように初期化する [FUN 2.4.3]。また、同じ理由で、*slip* の初期値は 0 [FUN 2.1] である。まとめると、初期イベント init は、初期モデルで定義した動作も含めて、以下のようになる。

init
$F := F_0$
$d := \frac{F_0}{m}$
$t := 0$
$V := V_0$
$x := 0$
$\omega_w := \frac{V_0}{r}$ [FUN 2.4.3]
$\omega_v := \frac{V_0}{r}$ [FUN 2.3.5]
$slip := 0$ [FUN 2.1]

時刻を Δt だけ進めるイベントは以下のようになる。

step
when
$0 < V$
then
$0 \leq F'$
$d' = \frac{F'}{m}$
$t := t + \Delta t$
$0 \leq V - d'\Delta t \Rightarrow V' = V - d'\Delta t$
$V - d'\Delta t < 0 \Rightarrow V' = 0$
$x' = x + V'\Delta t$
$0 \leq \omega'_w$ *[FUN 2.4.6]*
$\omega'_w \leq \omega'_v$ *[FUN 2.3.4]*
$\omega'_v = \frac{V'}{r}$ [FUN 2.3.4]
$slip := S - \frac{S\omega_w}{\omega_v}$ [FUN 2.1]
end

2.6 第 2 次精義化：μ-スリップ曲線

第 2 次精義化では、μ-スリップ曲線 [FUN 2.2.1] を導入する。μ-スリップ曲線は、スリップ率から摩擦率を得る関数である。私たちは、この曲線を折れ線で近似する（図 3）。

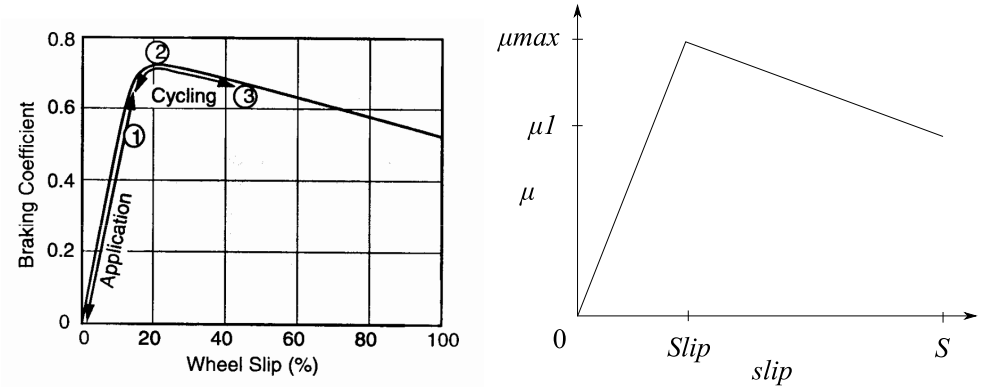

図 3　μ-スリップ曲線の概念図（左）と折れ線近似（右）

摩擦率の極大値を μ_{MAX}、摩擦率を極大にするスリップ率を *Slip* とする。また、スリップ率が 1（私たちのモデルでは $slip = S$）のときの摩擦率を μ_1 とする。これらの定数を用いて、μ-スリップ曲線は 3 点 $(0,0)$, $(Slip, \mu_{\mathrm{MAX}})$, (S, μ_1) を結ぶ折れ線で近似される。

なお、摩擦率を極大にするスリップ率は、経験的に 0.2 であるとされている [FUN 1.1]。私たちのモデルでは、これは公理 **axm2_5** に相当する。

定数: μ_{MAX}
定数: μ_1
定数: *Slip*

axm2_1: $0 < \mu_1$ *[FUN 2.2.1a]*
axm2_2: $\mu_1 < \mu_{\mathrm{MAX}}$ *[FUN 2.2.1b]*
axm2_3: $0 <$ *Slip [FUN 2.2.1c]*
axm2_4: *Slip* $< S$ *[FUN 2.2.1d]*
axm2_5: $Slip = \frac{S}{5}$ [FUN 1.1]

変数: μ

inv2_1: $0 \leq \mu$ *[FUN 2.2.1f]*
inv2_2: $\mu \leq \mu_{\mathrm{MAX}}$ *[FUN 2.2.1g]*
inv2_3: $\mu = 0 \iff slip = 0$ *[FUN 2.2.1h]*
inv2_4: $\mu = \mu_{\mathrm{MAX}} \iff slip = Slip$ *[FUN 2.2.1i]*
inv2_5: $slip = S \Rightarrow \mu = \mu_1$

システムの開始時にスリップ率は 0 である。μ-スリップ曲線で、スリップ率が 0 のとき摩擦率も 0 になる *[FUN 2.2.1h]* ので、摩擦率 μ の初期値は 0 *[FUN 2.2.1j]* である。

init
$F := F_0$
$d := \frac{F_0}{m}$
$t := 0$
$V := V_0$
$x := 0$
$\omega_w := \frac{V_0}{r}$
$\omega_v := \frac{V_0}{r}$
$slip := 0$
$\mu := 0$ *[FUN 2.2.1j]*

折れ線による近似は以下のようになる。

step
when
$0 < V$
then
$0 \leq F'$
$d' = \frac{F'}{m}$
$t := t + \Delta t$
$0 \leq V - d'\Delta t \Rightarrow V' = V - d'\Delta t$
$V - d'\Delta t < 0 \Rightarrow V' = 0$
$x' = x + V'\Delta t$
$0 \leq \omega'_w$
$\omega'_w \leq \omega'_v$
$\omega'_v = \frac{V'}{r}$
$slip := S - \frac{S\omega_w}{\omega_v}$
$slip' < Slip \Rightarrow \mu' = \frac{\mu_{\mathrm{MAX}} slip'}{Slip}$ *[FUN2.2.1k, l]*
$Slip \leq slip' \Rightarrow \mu' = \mu_{\mathrm{MAX}} - \frac{(\mu_{\mathrm{MAX}} - \mu_1)(slip' - Slip)}{S - Slip}$ *[FUN 2.2.1m, n]*
end

2.7 第 3 次精義化：トルクの導入

この精義化では、タイヤトルク T_t、ブレーキトルク T_b、正味トルク T_n、車輪の回転加速度 a_w、摩擦力 F_f、を導入する（図 4）。これらはいずれも変数である。また、定数として、車輪にかかる荷重 W と、車輪の回転慣性 I を導入する。なお、車輪にかかる荷重 W は、車両の質量ではなく、それに重力加速度を掛けたものである。

定数: W
定数: I
定数: ϵ

axm3_1: $0 < W$ *[ENV 2.2.2]*
axm3_2: $0 < I$ *[ENV 2.4.1]*
axm3_3: $F_0 = 0$ [FUN 2.2.2, FUN 2.3.1]
axm3_4: $\epsilon = W(\frac{r}{I} + \frac{1}{rm})\mu_{\mathrm{MAX}} \frac{S}{Slip}\Delta t$ *[FUN 3.2-3.4]*

自動車に後ろ向きにかかる力 F は摩擦力 F_f に等しい [FUN 2.3.1] ので、これを不変式 **inv3_8** に入れておく。

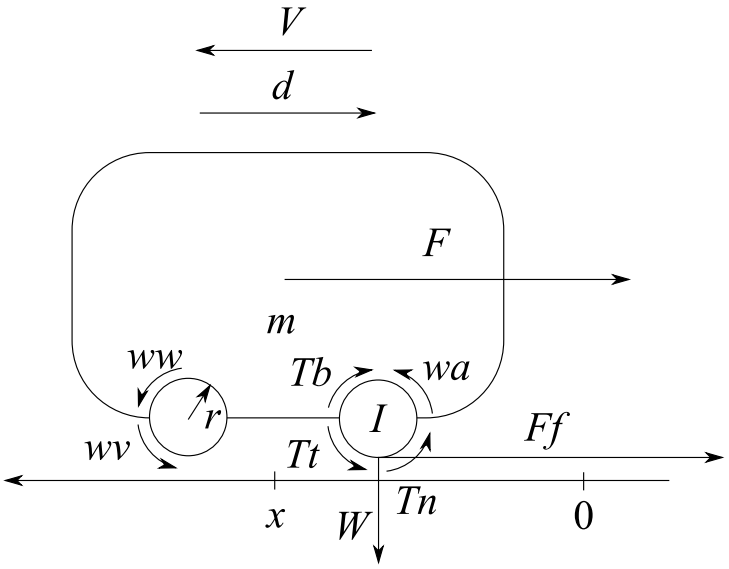

図 4　第 3 次精義化

変数: T_t
変数: T_b
変数: T_n
変数: a_w
変数: F_f

inv3_1: $T_t = rF_f$ [FUN 2.2.3]
inv3_2: $0 \leq T_t$ *[FUN 2.2.6]*
inv3_3: $0 \leq T_b$ *[FUN 2.1.4]*
inv3_4: $T_n = T_t - T_b$ [FUN 2.4.1]
inv3_5: $a_w = \frac{T_n}{I}$ [FUN 2.4.2]
inv3_6: $F_f = \mu W$ [FUN 2.2.2]
inv3_7: $0 \leq F_f$ *[FUN 2.2.5]*
inv3_8: $F = F_f$ [FUN 2.3.1]

システムの開始時にスリップ率は 0、また摩擦率 μ も 0 であることは以前の精義化で示した。ここでは、さらに、F_f の初期値も 0 [FUN 2.2.2] であることが分かる。すると、タイヤトルク T_t の初期値も 0 [FUN 2.2.3] である。また、ブレーキトルク T_b の初期値も 0 とすると、連鎖的に、正味トルク T_n と車輪加速度 a_w の初期値も 0 [FUN 2.4.1, FUN 2.4.2] である。ここで、$F = F_f$ であり、F の初期値は F_0、F_f の初期値は 0 なので、$F_0 = 0$ である。これを公理 **axm3_3** として定式化する。

init
$F := F_0$
$d := \frac{F_0}{m}$
$t := 0$
$V := V_0$
$x := 0$
$\omega_w := \frac{V_0}{r}$
$\omega_v := \frac{V_0}{r}$
$slip := 0$
$\mu := 0$
$T_t := 0$ [FUN 2.2.3]
$T_b := 0$ *[FUN 2.1.5]*
$T_n := 0$ [FUN 2.4.1]
$a_w := 0$ [FUN 2.4.2]
$F_f := 0$ [FUN 2.3.1]

時間を進行させるイベント step では、力 F を $F = F_f$ となるように更新する。また、車輪角速度 ω_w を車輪加速度 a_w の時間積分で表す [FUN 2.4.4]。ただし、スリップ率が $slip \leq S$ *[FUN 2.3]* を満たすためには、$0 \leq \omega'_w$ *[FUN 2.4.6]* である必要がある。そのため、時間積分の結果が 0 未満になるときは $\omega'_w = 0$ *[FUN 2.4.4a]* とする。

また、スリップ率が $0 \leq slip$ *[FUN 2.3]* を満たすためには、$\omega'_w \leq \omega'_v$ *[FUN 2.3.8]* である必要がある。これは、前時刻の ω_v が以下の式を満たすならば成立する[*5]。

$$W(\frac{r}{I} + \frac{1}{rm})\mu_{\mathrm{MAX}}\frac{S}{Slip}\Delta t \leq \omega_v \tag{3}$$

このうち $\mu_{\mathrm{MAX}}\frac{S}{Slip}$ は μ-スリップ曲線の原点付近の傾きである *[FUN 3.2]*。また、離散時間の単位 Δt を小さくすることで、この式の成立する条件を緩めることができる。ここで、左辺 $W(\frac{r}{I} + \frac{1}{rm})\mu_{\mathrm{MAX}}\frac{S}{Slip}\Delta t$ を定数 ϵ と置き直す *[FUN 3.4]*。そして、イベントのガード条件に $\epsilon \leq \omega_v$ *[FUN 3.5]* を加え、これが満たされないときはシステムを停止することにする。なお、これにより、ガード条件 $0 < V$ [FUN 3.1] は取り除くことができる。

さらに、ガード条件 $\epsilon \leq \omega_v$ の副産物として、$0 \leq V - d'\Delta t$ も証明できる。これにより、V の非決定的な定義 *[FUN 2.3.3a]* から条件分岐を取り除くことができる。

ω_w の計算方法が明確になったため、非決定的な動作 $0 \leq \omega'_w$ と $\omega'_w \leq \omega'_v$ は取り除かれる。同様に、$0 \leq F'$ も非決定的な動作から取り除く。F' は $F' = F'_f$ により決定されるからである。

step
when
$\epsilon \leq \omega_v$
then
$d' = \frac{F'}{m}$
$t := t + \Delta t$
$V' = V - d'\Delta t$
$x' = x + V'\Delta t$
$\omega'_v = \frac{V'}{r}$
$slip := S - \frac{S\omega_w}{\omega_v}$

[*5] この式の算出方法は本稿では省略する。

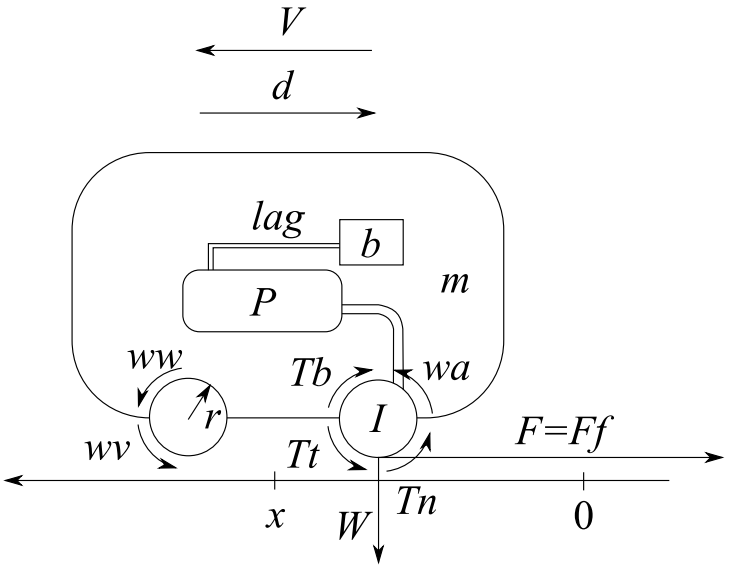

図 5　第 4 次精義化

$slip' < Slip \Rightarrow \mu' = \frac{\mu_{\mathrm{MAX}} slip'}{Slip}$
$Slip \leq slip' \Rightarrow \mu' = \mu_{\mathrm{MAX}} - \frac{(\mu_{\mathrm{MAX}} - \mu_1)(slip' - Slip)}{S - Slip}$
$T'_t = rF'_f$ [FUN 2.2.3]
$0 \leq T'_b$ *[FUN 2.1.4]*
$T'_n = T'_t - T'_b$ [FUN 2.4.1]
$a'_w = \frac{T'_n}{I}$ [FUN 2.4.2]
$F'_f = \mu' W$ [FUN 2.2.2]
$F' = F'_f$ [FUN 2.3.1]
$0 \leq \omega_w + a'_w \Delta t \Rightarrow \omega'_w = \omega_w + a'_w \Delta t$ [FUN 2.4.4]
$\omega_w + a'_w \Delta t < 0 \Rightarrow \omega'_w = 0$ [FUN 2.4.4]

end

2.8　第 4 次精義化：ブレーキ系

第 4 次精義化ではブレーキ系を導入する（図 5）。まず、ブレーキ系の入力値を b とする。この b の限界は定数 B で決められている。すなわち、$-B \leq b \leq B$ *[FUN 2.1.2c]* である。

入力値 b は、まず 1 次遅れに通される [FUN 2.1.2]。$u(k)$ を入力系列、$y(k)$ を出力系列、K と T を定数としたとき、1 次遅れの離散化は以下のようになる。

$$y(k) = (1 - \frac{\Delta t}{T}) y(k-1) + \frac{K \Delta t}{T} u(k-1) \tag{4}$$

私たちのモデルでは、1 次遅れの入力を b、出力を lag、定数を $lagT$ と $lagK$ と書き、以下のようになる。

$$lag := (1 - \frac{\Delta t}{lagT}) lag + \frac{lagK \Delta t}{T} b \tag{5}$$

ただし、$\Delta t \leq lagT$ *[FUN 2.1.2a]* でなければ、このシステムは破綻する。$\Delta t = lagT$ のときは $lag := lagKb$ となり、lag は b を 1 単位時間だけ遅らせたもの（の定数倍）になる。

続いて、ブレーキ圧力を P とすると、これは lag の時間積分で計算できる [FUN 2.1.2]。ただし、時間積分の結果が 0 未満になるときは、ブレーキ圧力は 0 とする *[FUN 2.1.2l]*。これを定数倍するとブレーキトルク T_b が得られる [FUN 2.1.3]。

定数: B	**axm4_1**: $0 < B$
定数: $lagT$	**axm4_2**: $\Delta t \leq lagT$ *[FUN 2.1.2a]*
定数: $lagK$	**axm4_3**: $0 < lagK$ *[FUN 2.1.2b]*
定数: K_f	**axm4_4**: $lagK \leq 1$ *[FUN 2.1.2b]*
	axm4_5: $0 < K_f$ *[ENV 2.1.1]*

変数: b	**inv4_1** $-B \leq b$ *[FUN 2.1.2c]*
変数: lag	**inv4_2** $b \leq B$ *[FUN 2.1.2c]*
変数: P	**inv4_3** $-B \leq lag$ *[FUN 2.1.2d]*
	inv4_4 $lag \leq B$ *[FUN 2.1.2d]*
	inv4_5 $0 \leq P$ *[FUN 2.1.2e]*
	inv4_6 $T_b = K_f P$ [FUN 2.1.3]

初期値は以下のように規定する。

init
- $F := F_0$
- $d := \frac{F_0}{m}$
- $t := 0$
- $V := V_0$
- $x := 0$
- $\omega_w := \frac{V_0}{r}$
- $\omega_v := \frac{V_0}{r}$
- $slip := 0$
- $\mu := 0$
- $T_t := 0$
- $T_b := 0$
- $T_n := 0$
- $a_w := 0$
- $F_f := 0$
- $b := B$ *[FUN 2.1.2f]*
- $lag := 0$ *[FUN 2.1.2g]*
- $P := 0$ [FUN 2.1.1]

時間を進行させるイベントは以下のようになる。T'_b の計算方法が明確になったため、前の精義化にあった $0 \leq T'_b$ は除いた。

step
when
- $\epsilon \leq \omega_v$

then
- $d' = \frac{F'}{m}$

$t := t + \Delta t$
$V' = V - d'\Delta t$
$x' = x + V'\Delta t$
$\omega'_v = \frac{V'}{r}$
$slip := S - \frac{S\omega_w}{\omega_v}$
$slip' < Slip \Rightarrow \mu' = \frac{\mu_{\mathrm{MAX}} slip'}{Slip}$
$Slip \leq slip' \Rightarrow \mu' = \mu_{\mathrm{MAX}} - \frac{(\mu_{\mathrm{MAX}} - \mu_1)(slip' - Slip)}{S - Slip}$
$T'_t = rF'_f$
$T'_n = T'_t - T'_b$
$a'_w = \frac{T'_n}{I}$
$F'_f = \mu' W$
$F' = F'_f$
$0 \leq \omega_w + a'_w\Delta t \Rightarrow \omega'_w = \omega_w + a'_w\Delta t$
$\omega_w + a'_w\Delta t < 0 \Rightarrow \omega'_w = 0$
$-B \leq b \wedge b \leq B$ *[FUN 2.1.2c]*
$lag' = (1 - \frac{\Delta t}{lagT})lag + \frac{lagK\Delta t}{lagT}b$ *[FUN 2.1.2h, i, j, k]*
$0 \leq P + lag'\Delta t \Rightarrow P' = P + lag'\Delta t$ *[FUN 2.1.2l]*
$P + lag'\Delta t < 0 \Rightarrow P' = 0$ *[FUN 2.1.2l]*
$T'_b = k_f P'$ [FUN 2.1.3]

end

2.9 第 5 次精義化：バンバン制御

この精義化ではバンバン制御を導入する。これはスリップ率 *slip* と、スリップ率の最適値 *Slip* の大小関係を見て、ブレーキ系の入力 b を最小値 $-B$ または最大値 B に設定する [FUN 1.2]。

この精義化で新たに導入する定数と変数はない。イベント step は以下のように変更する。

step
when
$\epsilon \leq \omega_v$
then
$d' = \frac{F'}{m}$
$t := t + \Delta t$
$V' = V - d'\Delta t$
$x' = x + V'\Delta t$
$\omega'_v = \frac{V'}{r}$
$slip := S - \frac{S\omega_w}{\omega_v}$
$slip' < Slip \Rightarrow \mu' = \frac{\mu_{\mathrm{MAX}} slip'}{Slip}$
$Slip \leq slip' \Rightarrow \mu' = \mu_{\mathrm{MAX}} - \frac{(\mu_{\mathrm{MAX}} - \mu_1)(slip' - Slip)}{S - Slip}$
$T'_t = rF'_f$
$T'_n = T'_t - T'_b$
$a'_w = \frac{T'_n}{I}$
$F'_f = \mu' W$
$F' = F'_f$
$0 \leq \omega_w + a'_w\Delta t \Rightarrow \omega'_w = \omega_w + a'_w\Delta t$

$\omega_w + a'_w \Delta t < 0 \Rightarrow \omega'_w = 0$
$lag' = (1 - \frac{\Delta t}{lagT})lag + \frac{lagK\Delta t}{lagT} b$
$0 \leq P + lag' \Delta t \Rightarrow P' = P + lag' \Delta t$
$P + lag' \Delta t < 0 \Rightarrow P' = 0$
$T'_b = k_f P'$
$slip' < Slip \Rightarrow b' = B$ [FUN 1.2]
$Slip \leq slip' \Rightarrow b' = -B$ [FUN 1.2]
end

2.10 ABS の有無による比較

これまでは、一連の精義化によって、ABS のモデルを作成してきた。この節では、ABS 有りと ABS 無しの 2 台の自動車のモデルを作り、両者を比較する。

まず、定数と公理は前節と同じである。また、変数も前節のものをそのまま利用する。それに加えて、2 台目の自動車のために、以下の変数を追加する。

変数: F_2
変数: d_2
変数: t_2
変数: V_2
変数: x_2
変数: ω_{w2}
変数: ω_{v2}
変数: $slip_2$
変数: μ_2
変数: T_{t2}
変数: T_{b2}
変数: T_{n2}
変数: a_{w2}
変数: F_{f2}
変数: b_2
変数: lag_2
変数: P_2

初期化イベント init には、2 台目の自動車のための変数を初期化する式を追加する。これは本稿では省略する。

時間を Δt だけ進行させるイベント step は、step1 と改名する。これは 1 台目の自動車の時間を進行させるイベントである。2 台目の自動車については、以下のイベントを用意する。

step2
when
$\epsilon \leq \omega_{v2}$
then
$d'_2 = \frac{F'_2}{m}$
$t_2 := t_2 + \Delta t$
$V'_2 = V_2 - d'_2 \Delta t$
$x'_2 = x_2 + V'_2 \Delta t$
$\omega'_{v2} = \frac{V'_2}{r}$
$slip_2 := S - \frac{S\omega_{w2}}{\omega_{v2}}$
$slip'_2 < Slip \Rightarrow \mu'_2 = \frac{\mu_{\mathrm{MAX}} slip'_2}{Slip}$
$Slip \leq slip'_2 \Rightarrow \mu'_2 = \mu_{\mathrm{MAX}} - \frac{(\mu_{\mathrm{MAX}} - \mu_1)(slip'_2 - Slip)}{S - Slip}$
$T'_{t2} = rF'_{f2}$
$T'_{n2} = T'_{t2} - T'_{b2}$

$a'_{w2} = \frac{T'_{n2}}{I}$
$F'_{f2} = \mu'_2 W$
$F'_2 = F'_{f2}$
$0 \leq \omega_{w2} + a'_{w2}\Delta t \Rightarrow \omega'_{w2} = \omega_{w2} + a'_{w2}\Delta t$
$\omega_{w2} + a'_{w2}\Delta t < 0 \Rightarrow \omega'_{w2} = 0$
$lag'_2 = (1 - \frac{\Delta t}{lagT})lag_2 + \frac{lagK\Delta t}{lagT}b_2$
$0 \leq P_2 + lag'_2\Delta t \Rightarrow P'_2 = P_2 + lag'_2\Delta t$
$P_2 + lag'_2\Delta t < 0 \Rightarrow P'_2 = 0$
$T'_{b2} = k_f P'_2$
$b_2 := B$
end

1 台目の自動車との違いは、ブレーキ系への入力 b_2 が最大値 B に固定されていることである。

最後に、証明すべき不変式には、以下のようなものが考えられる。

inv6_1 $\omega_v < \epsilon \wedge \omega_{v2} < \epsilon \Rightarrow t < t_2$	（ABS 有りの方が）早く停止する。
inv6_2 $\omega_v < \epsilon \wedge \omega_{v2} < \epsilon \Rightarrow x < x_2$	停止するまでに動く距離が短い。
inv6_3 $t = t_2 \Rightarrow \mu_2 \leq \mu$	同時刻で比較すると、常に摩擦力が大きい。
inv6_4 $t = t_2 \Rightarrow V < V_2$	同時刻で比較すると、常に速度が小さい。
inv6_5 $t = t_2 \Rightarrow x < x_2$	同時刻で比較すると、常に進んだ距離が短い。

これらの論理式が証明されれば、このモデルの ABS が正しく動作することが明らかになる。

3 まとめ

本稿では、ABS（アンチロック・ブレーキ・システム）を Event-B でモデル化した。また、Event-B のモデルの作成と証明を支援するソフトウェアである Rodin[*6]を用いて、半自動の証明を行った。その結果、第 2 次精義化までの全ての論理式と、第 5 次精義化までの主要な論理式を証明することができた。

Rodin では、全ての論理式を完全に自動的に証明することはできず、いくつかの論理式では人間がヒントを与える必要がある。そのため、手動の証明ほどではないとはいえ、証明には時間がかかる。半自動の証明支援プログラムを用いることの利点は、証明の時間を節約することの他に、証明それ自体が誤っていないことを客観的に確認できることである。

今回は、Rodin を用いて、第 5 次精義化までのほとんどの論理式を証明した。しかしながら、ABS の有無による比較（2.10 節）については、証明が著しく複雑である。そのため、本稿執筆時点では、この証明は実現していない。ただし、十分な手間と時間をかければ可能である。

Event-B の特徴は、システムが満たすべき性質を論理式で表現し、それを論理学的に証明することである。今回、証明の対象とした論理式は、変数の境界条件を与えるものが多数を占めている。例えば、摩擦率が負になることはあり得ないので、摩擦率 μ に対して $0 < \mu$ という不変式を追加して、これを証明している。変数の境界条件、特に「0 以上」か「0 より大きい」か、というような細かい部分について、厳密に証明が可能であることが分かった。今後、さらに十分な手間と時間をかければ、境界条件の他にも多数の有益な性質が証明できる。

一方で、Simulink などによるシミュレーションと比較すると、Event-B による証明では、特定の場合につい

[*6] http://rodin.cs.ncl.ac.uk/

てのシステム挙動が分からない。そのため、シミュレーションと証明は、必要に応じて使い分ける必要がある。

Event-B によるモデル作成と証明の過程で、もとの仕様書よりも詳細なモデルが得られた。特に、定数と変数の厳密な境界条件が得られた。このモデルの知見を、もとの仕様書にフィードバックすることで、仕様書をより正確にすることができる。さらに、この新しい仕様書をもとに Simulink でシミュレーションすることで、より正確なシミュレーションが可能になる。

今後の課題として、SLP 文書から Event-B のモデルへの自動変換プログラムの実現が挙げられる。仕様書をもとに SLP 文書を書くことは容易であるため、SLP から Event-B への自動変換が可能になれば、Event-B のモデル作成が容易になり、Event-B によるモデルの証明が利用しやすくなる。