Vol.2021-SE-209 No.5
2021/11/25

定量的モデル検査手法Model Measuringの実装に関する研究

小島 海[1]　高田 眞吾[1]

概要：システムの設計を表現するモデルを検証するための技術として，形式手法の一つであるモデル検査が挙げられる．従来のモデル検査では，モデルが仕様を満たすか否かという Bool 値及び，モデルが仕様を満たさないのであれば，反例に至るパスを出力していた．しかし，実際の開発現場ではこれらの情報だけでは不足が多く，それに伴い定量的な値を出力する定量的モデル検査手法が昨今提案されている．本研究では，これらの定量的モデル検査手法のうち，Henzinger らが提案した Model Measuring に注目する．Model Measuring のアイディアは実装されていないため，本研究ではこのアイディアを実装するための研究を行なった．

1. はじめに

システムの設計を表現するモデルを検証する手段として，形式手法の研究が進んでいる．システムの複雑性と重要性の増加に伴い，効果的な検証手法の必要性が高まっている [2] が，モデル検査 [1] はその一例であり，実際に使用されている形式手法の一つである．

典型的なモデル検査は, 対象とするモデルを状態遷移図で表し, またモデルが満たして欲しい仕様を時相論理式 (Linear Temporal Logic(LTL), Computation Tree Logic(CTL)) で表現し，モデルが仕様を満たしているか否かを判定する．近年，このような 2 値の出力をするモデル検査を拡張し，モデルの仕様の満足度合いを定量的に出力する技術が研究されている [2]．その中の一つである Model Measuring[3] に本論文では注目する．

Model Measuring では，モデル間の距離を擬似的に測定する関数が定義済みであることを前提とする．この距離関数を用いて，Model Measuring は次の質問の答えを出力する．

Model Measuring: モデル M と仕様 ϕ が与えられた時，M からの距離が ρ 以内である全てのモデル M' が ϕ を満たすとする．このような ρ の最大値は何か．

図 1 に Model Measuring の概念図を示す．図中の $d_M(M')$ とは，モデル M から M' の距離を測定する一引数の距離関数であり，本論文では [3] を参考にして，この関数を similarity measure と呼ぶ．また，先の質問の答えである最大距離を stability radius と呼ぶ．モデル M からの距離が ρ 以内にある全てのモデル M' が仕様 ϕ を満たす時，M は ρ だけ摂動しても仕様を満たすことを意味する．

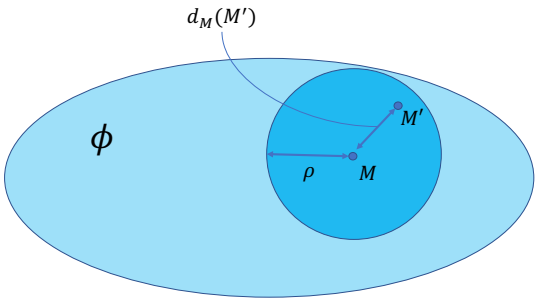

図 1　Model Measuring: 仕様 ϕ に対するモデル M の stability radius ρ

Model Measuring は古典的なモデル検査の一般化であり，特にモデルの堅牢性を測定することができる．現に，[3] では，堅牢性や仕様の満足度などの概念を計算する問題に適用できる例が示されている．

Model Measuring のフレームワークは，オートマトンを基本としたモデル検査手法 [4][5][6] をベースとして提案されている．オートマトンベースの一般的なモデル検査では，次のような手順で行うことが多い．ここで，検証対象のモデルを状態遷移図 M，仕様を ϕ とする．

(1) M を受理するオートマトン A_M を構成する．
(2) $\neg\phi$(ϕ の否定) をオートマトン $A_{\neg\phi}$ に変換する．

[1] 慶應義塾大学大学院 理工学研究科

(3) A_M と $A_{\neg\phi}$ から，直積 $A_M \times A_{\neg\phi}$ を求める．
(4) $A_M \times A_{\neg\phi}$ が受理するワードを探索する．

(4) のステップを，本論文では [3] を参考にして emptiness question と呼ぶ．emptiness question の結果，オートマトンが受理するワードが一つでもあれば，M は仕様 ϕ を満たさないことを出力し，オートマトンが受理するワードが一つもなければ，M は仕様 ϕ を満たすことを出力する．

Model Measuring で核となるのは，上記のオートマトンベースのモデル検査の手順 (4) のステップを，emptiness question から optimal-weight question に置き換える点である．これは，オートマトンが受理する全てのワードの重みを計算し，それの最小値を求める問題である．Model Measuring の意味や手順については後述する．

Model Measuring は現時点ではフレームワークのみが提案されており，そのまま実装はできない．そこで本論文では，実装するために不足している部分を明らかにし，そのための各手順のアルゴリズムを与える．特に optimal-weight question に対するアルゴリズムは，emptiness question に対するアルゴリズムから定義した．また，[3] では，仕様の表現方法やオートマトンの種類について一般化したものを扱っているが，この論文では仕様の表現に LTL を，オートマトンの種類に non-deterministic Büchi Automata を採用した．

以下，本論文ではまず 2 章で，emptiness question に対する既存のアルゴリズムと，定量的モデル検査に関して紹介をする．3 章ではモデル検査，4 章では Model Measuring の定義とそのための準備についてそれぞれ説明し，それを元に 5 章で提案アルゴリズムと実装について説明する．最後 6 章で本論文をまとめる．

2. 関連研究

emptiness question に対するアプローチは大きく分けて 2 つあり，それらは NDFSs(Nested depth-first searched) を使用する方法と，グラフの強連結成分 (SCCs: Strongly Connected Components) の計算を用いる方法である．NDFSs を使用する方法は [8] で提案され，Holzmann らはそれを改良することで汎用モデル検査ツール Spin を提案した [7][9]．また，SCCs の計算を用いる方法としては，[11][12][13][10] で提案，改良されている．本論文では，NDFSs を採用した．

2 値を出力する典型的なモデル検査に対して，定量的な値を出力する定量的モデル検査手法は Model Measuring 以外も多く提案されている．定量的モデル検査の出力値を比較することにより，共通の仕様を元に作成された異なる 2 つのモデル間の比較に役立つことが期待されている．これは仕様を満たすモデル間以外にも，仕様を満たさないモデル間に適用することで，どれくらい仕様を満たしていれば妥協できるか，という”best effort”の面でも利用できると考えられている．以下に，モデル検査の定量的な拡張の例を挙げる．

[14] では，定量的な値を組み込むことによる，時相論理の拡張 (quantitative temporal logic) が提案されている．また，確率を考慮するシステムに対し，モデルが仕様を満たす絶対的な保証ではなく，確率的な保証をする Statistical Model Checking という手法も提案され，またそれに partial order reduction を組み込んだ場合の検証もされている [15][16]．本論文で注目する Model Measuring の技術は，2 つのモデル間の距離という定量的な要素を組み込んでおり，上記の研究とは違うアプローチでモデル検査の定量的な拡張を図っている．

システム間の距離をシミュレーションゲームの結果として定義した [17] は，本論文の距離関数に応用できる．また，Model Measuring のフレームワークを離散システムやハイブリッドシステムに適用したものも提案されている [18]．本論文の実装を応用することで，離散システムやハイブリッドシステムに適用した実装を与えることも可能だと考えられる．

3. モデル検査

この章では，本論文におけるモデル検査の定義を述べる．3.1 節ではそのために必要な準備から述べる．

3.1 準備

Nondeterministic Büchi Automata は，$(\sum, Q, Q_0, \delta, F)$ で構成される．それぞれの要素は次で定義される．

- $\sum$: 記号の有限集合 (アルファベット)
- Q: 状態の有限集合
- $Q_0 \subseteq Q$: 初期状態の有限集合
- $\delta \subseteq Q \times \sum \times Q$: 状態の遷移関係
- $F \subseteq Q$: 終了状態の有限集合

Nondeterministic Büchi Automata A における記号列 $w = a_1 a_2 \cdots$ に対応するパス π は，$\pi(0) \in Q_0$ かつ，$i \in [1, \infty)$ に対して $(q_{i-1}, a_i, q_i) \in \delta$ を満たすような状態の列を指す．なお，$n \in \mathbb{N}$ に対し，$\pi(n)$ は，π の n 番目の状態を指す．また，この記号列 w を，本論文では [3] を参考にしてワードと呼ぶ．

Nondeterministic Büchi Automata が受理するワードは，無限に続く記号列 (ω ワード) である．なぜなら Nondeterministic Büchi Automata の受理条件が，「ワードに対応するパスの中に無限回 $f \subseteq F$ が出現すること」であるためである．Nondeterministic Büchi Automata A が受理する全

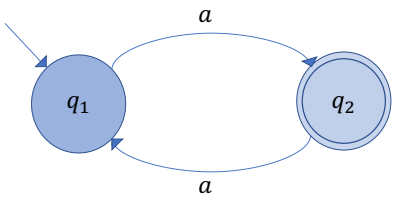

図 2 Nondeterministic Büchi Automata A_1

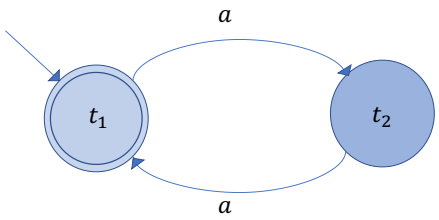

図 3 Nondeterministic Büchi Automata A_2

てのワードの集合を，$L(A)$ で表す．

例えば，図 2 のような Nondeterministic Büchi Automata A_1 を考える．$A_1 = (\sum, Q_{A_1}, Q_{0,A_1}, \delta_{A_1}, F_{A_1})$ は $Q_{A_1} = \{q_1, q_2\}, Q_{0,A_1} = \{q_1\}, F_{A_1} = \{q_2\}$ 及び $\delta(q_1, a) = q_2, \delta(q_2, a) = q_1$ で定義される．A_1 が受理するパスは，q_2 が無限回出現するパス $q_1q_2q_1q_2\cdots$ となるため，ワード $aa\cdots(= a^\omega)$ を受理する．よって，$L(A_1) = \{aa\cdots\}$ である．

2 つの Nondeterministic (Büchi) Automata $A_1 = (\sum_1, Q_1, Q_{0,1}, \delta_1, F_1), A_2 = (\sum_2, Q_2, Q_{0,2}, \delta_2, F_2)$ の直積 $A_1 \times A_2 = (\sum, Q, Q_0, \delta, F)$ は次で定義される．(なお 2 つのオートマトンで用いられるアルファベットは共通する．)

- $Q = Q_1 \times Q_2 \times \{1, 2\}$
- $Q_0 = Q_{0,1} \times Q_{0,2} \times \{1\}$
- $\delta((q_1, q_2, c), \sigma) = \delta_1(q_1, \sigma) \times \delta_2(q_2, \sigma) \times \{next(q_1, q_2, c)\}$
  $(q_1 \in Q_1,\ q_2 \in Q_2,\ , c \in \{1, 2\}, \sigma \in \sum)$
  ここで，

$$next(q_1, q_2, c) = \begin{cases} 1 & if (c = 1\ and\ q_1 \notin F_1)\ or\ (c = 2\ and\ q_2 \in F_2) \\ 2 & if (c = 1\ and\ q_1 \in F_1)\ or\ (c = 2\ and\ q_2 \notin F_2) \end{cases}$$

- $F = F_1 \times Q_2 \times \{1\}$

ここで，$1, 2, 1$ という記述をしたが，これは 2 つの Büchi Automata の直積を Büchi Automata として扱えるようにするための，添え字である．例えば，$Q_1 = \{q_1\}, Q_2 = \{q_2\}$ であれば，$Q = \{(q_1, q_2, 1), (q_1, q_2, 1)\}$ となる．

A_1 と A_2 の直積 $A_1 \times A_2$ に対して，$L(A_1 \times A_2) = L(A_1) \cap L(A_2)$ が成り立つ．

例えば，図 2，図 3 のような Nondeterministic Büchi Automata A_1, A_2 の直積 $A_1 \times A_2$ は図 4 のようになる．$L(A_1) = \{a^\omega\}, L(A_2) = \{a^\omega\}$ であり，$L(A_1 \times A_2) = \{a^\omega\}$ であるため，$L(A_1 \times A_2) = L(A_1) \cap L(A_2)$ が成り立っていることがわかる．

続いて，仕様を表現する LTL 式について説明をする．本論文では，LTL 式を用いたモデル検査及び Model Measuring を行う．LTL 式は原始論理式の集合 AP 上に，以下のように再帰的に定義される記号列である．

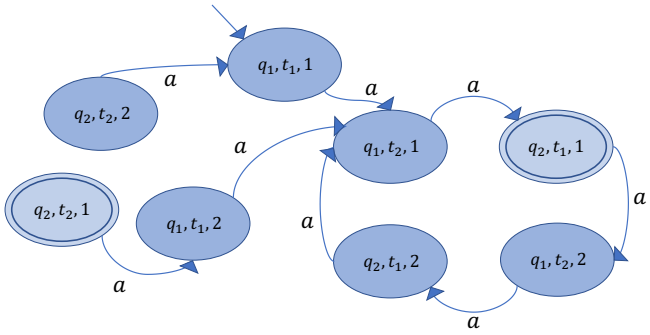

図 4 Nondeterministic Büchi Automata $A_1 \times A_2$

- $true$, $false$, p $(p \in AP)$ は LTL 式
- ϕ_1, ϕ_2 が LTL 式の時，$\neg\phi_1, \phi_1 \wedge \phi_2, X\phi_1, \phi_1 U \phi_2$ は LTL 式

LTL 式にはこれらの記号の他に，便利のため F, G, R を用いることが多いが，これらは全て上の記号によって定義できる．

LTL 式は，モデルのパスに対して，評価を行うためによく用いられる．パス $path = \sigma_1\sigma_2\cdots(\sigma_i$ はモデルの状態集合の要素) が LTL 式 ϕ を満たすことを，$path \vDash \phi$ と書き次で定義される．ここで，$n \in \mathbb{N}$ に対し，$path^n = \sigma_n\sigma_{n+1}\cdots$ とする．

- 任意の $path$ に対し，$path \vDash true$, $path \nvDash false$
- 状態 σ_1 で $p \in AP$ が成り立つ時，$path \vDash p$
- LTL 式 ϕ_1 に対し，$path \nvDash \phi_1$ の時，$path \vDash \neg\phi_1$
- LTL 式 ϕ_1, ϕ_2 に対し，$path \vDash \phi_1$ かつ $path \vDash \phi_2$ の時，$path \vDash \phi_1 \wedge \phi_2$
- LTL 式 ϕ に対し，$\phi \vDash path^2$ であれば，$path \vDash X\phi$
- LTL 式 ϕ_1, ϕ_2 に対し，任意の $i(1 \leq i \leq k)$ に対し $path^k \vDash \phi_2 \wedge path^i \vDash \phi_1$ を満たすような $k \leq 1$ が存在する時，$path \vDash \phi_1 U \phi_2$

また，これらに加えて次で定義される記号もよく用いられる．

- $F\phi = true\ U\ \phi$
- $\phi_1 F \phi_2 = \neg(\neg\phi_1\ U\ \neg\phi_2)$

- $G\phi = false\ R\phi$

次の節 3.2 では，これらを用いてモデル検査を説明する．

3.2 モデル検査

検証対象システムを表すモデルを M，モデルに期待される性質 (仕様) を ϕ とする．ここで，M は状態遷移図，ϕ は時相論理 (ここでは特に線形時相論理 LTL) とする．

その上でモデル検査とは，「M は仕様 ϕ を満たすか否か」を決定する問題と定義する．つまりは，$M \vDash \phi$ が成り立つか否かを決定する問題と言える．

この決定問題に対する，オートマトンベースの手順は 1 章で述べた通り，(1)M を受理するオートマトン A_M の構成，(2)$\neg\phi$ から $A_{\neg\phi}$ への変換，(3) 直積 $A_M \times A_{\neg\phi}$ を作成，(4)$A_M \times A_{\neg\phi}$ に対する emptiness question からなる (図 5)．

ここで，(2) において ϕ ではなく $\neg\phi$ を用いるのは，仕様を満たすパスを発見するのではなく，仕様を満たさないパスを発見することがモデル検査の目的として多いためである．$\neg\phi$ を用いることにより，仕様を満たさないパスが存在するか否かという決定問題にすることができる．

(2) のオートマトン $A_{\neg\phi}$ には，Büchi Automata がよく用いられる．LTL 式を Büchi Automata に変換する手法は [19] で提案されており，[4] によくまとめられている．

また，(3) における $A_M \times A_{\neg\phi}$ は，Büchi Automata になる．

4. Model Measuring

この章では，本論文における Model Measuring の定義を述べる．4.1 節ではそのために必要な準備を述べる．

4.1 準備

Nondeterministic Weighted Büchi Automata A は，$(\sum, Q, Q_0, \delta, F, C)$ で構成される．$\sum, Q, Q_0, \delta, F$ の定義は，3.1 節の Nondeterministic Büchi Automata の定義と同様である．$C : \delta \mapsto \mathbb{N}$ は，遷移関係に対し自然数で表される重みを与える関数である．

Weighted Scheme f は，Nondeterministic Weighted Büchi Automata 上のパスに対し，その重みを計算する関数の集合である．[3] では，4 つの関数 $SUM, MAX, DISC_\lambda, LIMAVG$ を下のように定義している．なお，π は Nondeterministic Weighted Büchi Automata におけるパスとし，$wt(\pi, i)$ は，π における i 番目の遷移における重みとする．

- $SUM(\pi) = \sum_{i=1}^{\infty} wt(\pi, i)$
- $MAX(\pi) = max_{i=1}^{\infty} wt(\pi, i)$
- $DISC_\lambda(\pi) = (1-\lambda)\sum_{i=1}^{\infty} \lambda^i wt(\pi, i)\ (\lambda \in (0, 1))$
- $LIMAVG(\pi) = lim\ inf_{k\to\infty} \frac{1}{k} \sum_{i=1}^{k} wt(\pi, i)$

Nondeterministic Weighted Büchi Automata A 上のワード w の，Weighting Scheme f による重みは，ワードに対応するパス π の f による重みであり，$A^f(w)$ で表す．ただし A に受理されないパスの重みは，∞ とする．また，以降 f が特定の関数を指していない場合，$A^f(w)$ を $A(w)$ と略記することがある．

Nondeterministic Weighted Büchi Automata A, Weighting Scheme f が与えられた時，A に対する optimal-weight question とは，A が受理する全てのワードに対する $A^f(w)$ の最小値を計算する問題とする．optimal-weight question の計算量に関しては，[3] を参照されたい．

$A^f(w)$ 及び optimal-weight question を上記のように定義することで Model Measuring を解くことができる．これらを用いて Model Measuring の手順を求める方法に関しては，補遺 A に示す．

次の 4.2 節では，これらを用いて Model Measuring を定義する．

4.2 Model Measuring

Model Measuring の一般的な定義と，LTL 式を用いた場合について述べる．

モデル M，仕様 P，similarity measure d_M が与えられた時，Model Measuring は，1 章で述べた通り次の質問の答えを求める問題である．

Model Measuring: モデル M と仕様 ϕ が与えられた時，M からの距離が ρ 以内である全てのモデル M' が ϕ を満たすとする．このような ρ の最大値は何か．

この質問の答えを stability radius $sr_d(M, P)$ とする．この問題は次のように定式化できる．

- $if\ M \vDash P, sr_d(M, P) = sup\{\rho \le 0 : \forall M'(d_M(M') < \rho \Rightarrow M' \vDash P)\}$
- $if\ M \vDash \neg P, sr_d(M, P) = sr_d(M, \neg P)$
- $otherwise, sr_d(M, P) = 0$

M が P を満たしている場合は，M から距離 ρ 以内にある全てのモデルが P を満たすような ρ を考える．そのような距離 ρ の最大値が stability radius である．

また，stability radius $sr_d(M, P)$ は $[0, \infty]$ の値を取るが，次のような計算を行うことで $[0, 1]$ の値を取るように正規化することができる．これにより得られる値を $[P]_{d_M}$ とする．

- $if\ M \vDash P, [P]_{d_M} = 1 - 2^{-sr_{d_M}(M,P)-1} \quad \in ((\frac{1}{2}, 1])$
- $if\ M \vDash \neg P, [P]_{d_M} = 1 - [\neg P]_{d_M} \quad \in ([0, \frac{1}{2}))$
- $otherwise, [P]_{d_M} = \frac{1}{2}$

仕様に LTL 式を用いた場合，次のような手順で stability radius を求めることができる (図 6)．モデル M, 仕様 ϕ,

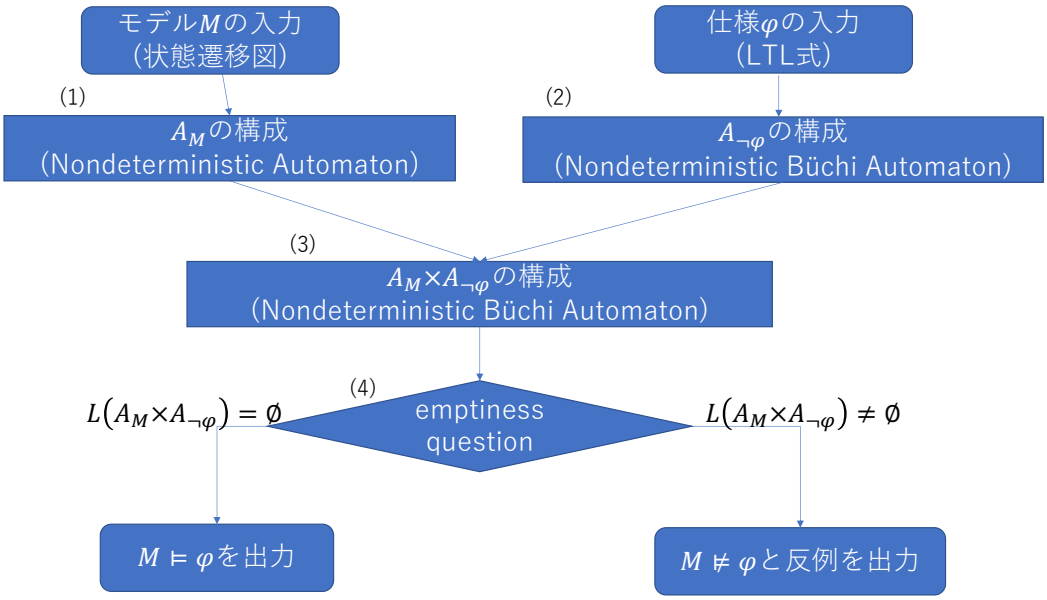

図 5 モデル検査の手順

similarity measure d_M, Weighting Scheme f が与えられた時,

(1) M と d_M から Nondeterministic Weighted Büchi Automata A_{dist} を構成する.
(2) $\neg\phi$(ϕ の否定) から $A_{\neg\phi}$ に変換する.
(3) A_{dist} と $A_{\neg\phi}$ から直積 $A_{dist}\times A_{\neg\phi}$ を求める.
(4) f を用いて, $A_{dist}\times A_{\neg\phi}$ に対する optimal-weight question を計算する. ($sr_d(M,\phi)$ を得る.)
(5) $[\phi]_{d_M}$ を計算する.

Model Measuring の手順 (1) において, A_{dist} は次を満たすように定義する.

$$d_M(M') = sup\{A_{dist}(w) : w \ is \ a \ word \ of \ M'\}$$

Model Measuring の手順 (2) において, モデル検査の手順 (2) では Nondeterministic Büchi Automata に変換したが, Model Measuring では Nondeterministic Weighted Büchi Automata という重み付きのオートマトンに変換している. これは, モデル検査と同様に Nondeterministic Büchi Automata に変換した後, その全ての遷移関係の重みを 0 とすることにより得られる. つまり, $A_{\neg\phi}$ 中の各遷移の重みは 0 である. よって, (3) の直積で得られる $A_{dist}\times A_{\neg\phi}$ での遷移関係での重みは全て, A_{dist} から得られるものである.

なお, LTL を用いた Model Measuring の手順がこのようになることは, 補遺 A で記述する.

5. 実装

[3] では, 4.2 節で述べた手順が提案されており, どのように各手順の計算を行うかは明記されていない. 本論文ではこれらの各手順に実装を与え, 本章ではどのように実装したかを記す.

5.1 $A_{\neg\phi}$ の構成 (手順 (2))

LTL から Nondeterministic Büchi Automata に変換する手法は, LTL2BA[*1]を用いた. LTL2BA は, [20] の手法を採用した LTL から Büchi Automata に変換するツールである.

$\neg\phi$ を LTL2BA に入力し, 得られた Büchi Automata の各遷移に重み 0 を与えて, $A_{\neg\phi}$ を得ることができる.

例えば $p, q \in AP$ とした時, LTL 式 $\neg FG(P\wedge\neg Q)$(直感的には p がずっと成り立つならばいずれ q が成り立つ, という弱公平性を表す) に対する Weighted Büchi Automata は図 7 のようになる. 2 つの状態 $0, 1$ があり, それらには合計 4 つの遷移がある. それぞれの遷移は σ, w がラベリングされており, σ は遷移条件, w は重みを表している. 先述した通り, $A_{\neg\phi}$ の各遷移の重みは全て 0 である.

5.2 $A_{dist}\times A_{\neg\phi}$ の構成 手順 (3)

4.1 節の Nondeterministic Büchi Automata の直積の定義を元にし, 新たに Nondeterministic Weighted Büchi Automata の直積を定義し, 実装を行った. 具体的には,

$$A_{dist} = (\sum, Q_{dist}, Q_{0,dist}, \delta_{dist}, F_{dist}, C_{dist}),$$
$$A_{\neg\phi} = (\sum, Q_{\neg\phi}, Q_{0,\neg\phi}, \delta_{\neg\phi}, F_{\neg\phi}, C_{\neg\phi})$$

に対し,

$$A_{dist}\times A_{\neg\phi} = (\sum, Q, Q_0, \delta, F, C)$$

[*1] http://www.lsv.fr/ gastin/ltl2ba/

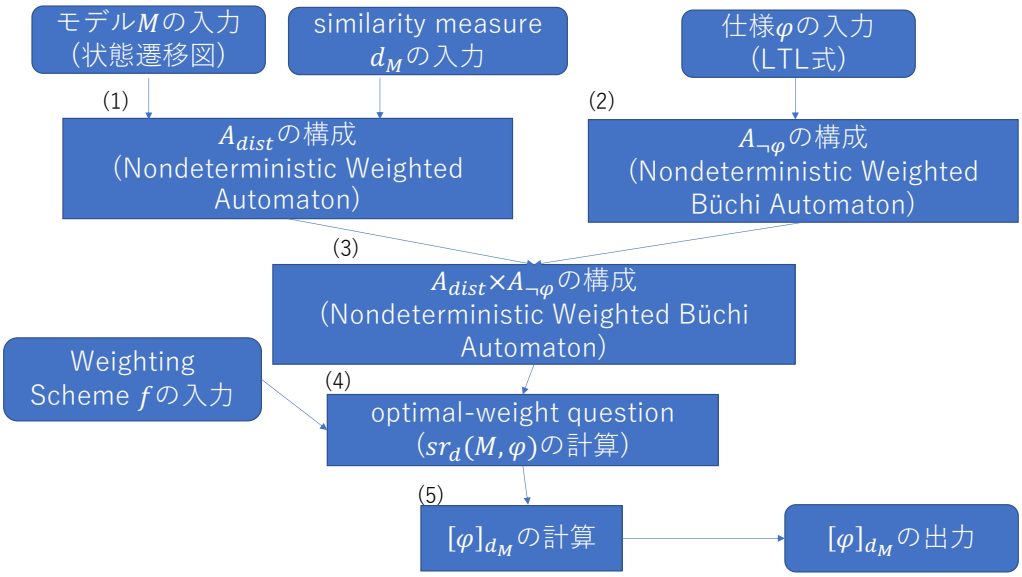

図 6 Model Measuring の手順

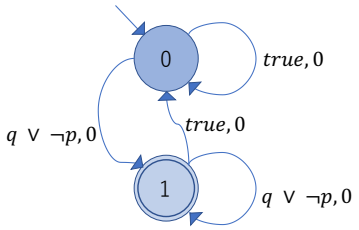

図 7 $\neg FG(P \wedge \neg Q)$ から変換された Weighted Büchi Automata

を次のように定義する．

- $Q = Q_{dist} \times Q_{\neg\phi} \times \{1, 2\}$
- $Q_0 = Q_{0,dist} \times Q_{0,\neg\phi} \times 1$
- $\delta((q_{dist}, q_{\neg\phi}, c), \sigma) =$
  $\delta_{dist}(q_{dist}, \sigma) \times \delta_{\neg\phi}(q_{\neg\phi}, \sigma) \times next(q_{dist}, q_{\neg\phi}, c)$
  $(q_{dist} \in Q_{dist}, q_{\neg\phi} \in Q_{\neg\phi}, c \in \{1, 2\})$
  ここで，

  $next(q_{dist}, q_{\neg\phi}, c) =$

  $$\begin{cases} 1 & if (c = 1 \ and \ q_{dist} \notin F_{dist}) \ or \ (c = 2 \ and \ q_{\neg\phi} \in F_{\neg\phi}) \\ 2 & if (c = 1 \ and \ q_{dist} \in F_{dist}) \ or \ (c = 2 \ and \ q_{\neg\phi} \notin F_{\neg\phi}) \end{cases}$$

- $F = F_{dist} \times Q_{\neg\phi} \times \{1\}$
- $C((q_{dist}, q_{\neg\phi}, c), \sigma, (q'_{dist}, q'_{\neg\phi}, next(q_{dist}, q_{\neg\phi}, c))) =$
  $C_{dist}(q_{dist}, \sigma, q'_{dist})$

ここで，$\sum$ は 3 つのオートマトンで共通である．$C_{\neg\phi}$ はどのような入力に対しても 0 を返す関数であるから，C による重み付けは全て C_{dist} を参照するようにした．

5.3 optimal-weight question 手順 (4)

2 章で述べた通り，emptiness question に対するアプローチは大きく 2 つあり，optimal-weight question の手順には NDFSs をベースに採用した．emptiness question ではパスを最低 1 つ見つけることが目的だが，optimal-weight question では受理するワードを全探索する必要があるためである．

具体的には，Nondeterministic Weighted Büchi Automata A と Weighting Scheme$f$ を入力とし，次の手順を踏む．

(1) NDFSs を用いて A が受理するパスを全探索し，パスの集合 $\prod$ を得る．
(2) $\prod$ の各要素 π に対し，f を適用することで重みの集合 W を得る．
(3) W の最小値を出力する．

これにより出力された値が，モデル M の仕様 ϕ に対する stability radius となる．ただし．(1) の過程で $\prod = \emptyset$ であった場合，Model Measuring の手順 (2) における ϕ を $\neg\phi$ に置き換えて再度繰り返し計算をした．

5.4 A_{dist} の構成 手順 (1)

最後に，A_{dist} の構成について述べる．本論文では A_{dist} の構成は手作業で行うこととした．以下にその理由を述べる．

まず，similarity measure は，Model Measuring で測定したい対象を踏まえて，ユーザが決定しなければならない．例えば [3] の TCP ハンドシェイクプロトコルの例では，モデル N を信頼できるチャネルにおけるプロトコルをモデリングしたものとし，モデル M を実行の間に最大 k 回の

パケットロスをするプロトコルをモデリングしたものとした．その上で $d_N(M) = k$ と定め，プロトコルの停止性を仕様 (性質) として Model Measuring を行うことによって，プロトコルの停止性が保証される最大のパケットロス数を測定している．

A_{dist} の構成には，ハイパーバイザー H を用いる方法が提案されている [3]．この方法では測定したい対象に応じてハイパーバイザーを適切に設定する必要があり，その例や構成方法の手引きは今後の研究対象である．

6. 結論

本論文では，モデル検査と Model Measuring の手順を比較し，Model Measuring のフレームワークに対してアルゴリズムを与え，実装を行なった．A_{dist} の構成にあたっては，測定したい対象に応じて適切な similarity measure 及びハイパーバイザーを与える必要があり，本論文では手作業で行うものとした．この手順のアルゴリズム化 (あるいは手引きの作成) は今後の課題である．

また，本論文では特にモデル検査器 Spin と類似したアルゴリズムを選択したので，今後 Spin 上に Model Measuring を実装できることが期待される．Model Measuring は典型的なモデル検査の一般化に留まらず，他の定量的モデル検査も含有するため，その面でも汎用的なモデル検査器とともに使用されることが期待できる．

参考文献

[1] Clarke, E., Grumberg, O., Peled, D.: *Model Checking*, The MIT Press, 1999.
[2] Clarke, E., Henzinger T., Veith, H.: *Introduction to model checking*, Handbook of Model Checking. Springer, pp. 1-26, 2018.
[3] Henzinger, T., Otop, J.: *From model checking to model measuring*, D' Argenio, P.R., Melgratti, H. (eds.) CONCUR 2013 – Concurrency Theory. LNCS, vol. 8052, pp. 273–287. Springer, Heidelberg, 2013.
[4] Kupferman, O.: *Automata Theory and Model Checking*, Handbook of Model Checking. Springer, pp. 107-152, 2018.
[5] Holzmann, G.: *Explicit-State Model Checking*, Handbook of Model Checking. Springer, pp.153-171, 2018.
[6] M,Vardi.: *An Automata-Theoretic Approach to Linear Temporal Logic*, volume 1043 of Lecture Notes in Computer Science, Springer, pp.238-266, 1996.
[7] Holzmann, G.: The model checker SPIN. Software Engineering 23, pp.279-295, 1997.
[8] Courcoubetis, C., Vardi, M., Wolper, P., Yannakakis, M.: *Memory-efficient algorithm for the verification of temporal properties*, Methods Syst, pp.275-288, 1992.
[9] Holzmann, G., Peled, D., Yannakakis, M.: *On nested depth first search*, SPIN'96, volume 32 of DIMAXS, 1996.
[10] Couvreur, J., Duret-Lutz, A., Poitrenaud, D.: *On-the-fly emptiness checks for generalized Büchi automata*, SPIN'05, volume 3639 of LNCS, PP.143-158, 2005.
[11] Geldenhuys, J., Valmari, A.: *Tarjan's algorithm makes on-the-fly LTL verification more efficient*, TACAS'04, volume 2988 of LNCS, pp.205-219, 2004.
[12] Hammer, M., Knapp A., Mers, S.: *Truly on-the-fly LTL model chekcing*, TACAS'05, LNCS, 2005.
[13] Geledenhuys, J., Valmari, A.: *More efficient on-the-fly LTL verification with Tarjan's algorithm*, Theoretical Computer Science, 2005.
[14] Boker, U., Chatterjee, K., Henzinger, T., Kupferman, O,: *Temporal specification with accumulative values*, ACM Trans. Comput, 2014.
[15] Legay, A., Delahaye, B., Bensalem, S.: *Statistical model checking: an overview*, RB, LNCS, volume 6418, pp.122-135, 2010.
[16] Bogdoll, J., Fioriti, LMF., Hartmanns, A., Hermanns, H.: *Partial order methods for statistical model checking and simulation*, FMOODS/FORTE, LNCS, volume 6722, pp.59-74, 2011.
[17] Cerny, P., Henzinger, T, Radhakrishna, A.: *Simulation distances*, Theor. Comput. Sci. pp.21-35, 2012.
[18] Henzinger, T., Otop, J.: *Simulation Distances*, Nonlin. Anal.: Hybr. Syst. 23, Supplement C, pp.166-190, 2017.
[19] Vardi, M., Wolper, P.: *Reasoning about Infinite Computations*, Comput. 115(1), pp.1-37, 1994.
[20] Gastin, P., Oddoux, D.: *Fast LTL to Büchi autimata translation*, Proceeding of the 13th International Conference on Computer-Aided Verification. Lecture Notes in Computer Science, volume 2102, 2001.

付　　録

補遺 A　Model Measuring の手順の得方

ここでは，Model Measuring の定義から，LTL を用いた Model Measuring の手順を得る方法について説明する．つまり，モデル M, 仕様 ϕ に対し，$M \vDash \phi$ の時，

$$sr_d(M,\phi) = sup\{\rho \leq 0 : \forall M'(d_M(M') < \rho \Rightarrow M' \vDash \phi)\} \tag{A.1}$$

及び

$$d_M(M') = sup\{A_{dist}(w) : w\ is\ a\ word\ of\ M'\} \tag{A.2}$$

から，

$$optimal - weight\ question :$$
$$sr_d(M,\phi) =$$
$$inf\{A_{dist} \times A_{\neg\phi}(w) : w\ is\ a\ word\ of\ A_{dist} \times A_{\neg\phi}\} \tag{A.3}$$

で $sr_d(M,P)$ を求められることを説明する．

まず，ワード w が $A_{\neg\phi}$ に受理される場合，

$$A_{dist} \times A_{\neg\phi}(w) = A_{dist}(w)$$

である．M との距離が k である任意のモデル M_k を考える．つまり，

$$d_M(M^k) = k$$

であり，M_k の任意のワード w_k に対し，(A.2) より，

$$A_{dist}(w_k) \leq k$$

である．$M_k \models \phi$ である時，M_k には $A_{\neg\phi}$ に受理されるワード w'_k が存在して，

$$A_{dist} \times A_{\neg\phi}(w'_k) = A_{dist}(w'_k)$$

かつ，(A.1) より

$$sr_d(M, \phi) \leq k$$

である．このような k の最小値が $sr_d(M, \phi)$ と一致するため，(A.3) のように $A_{dist} \times A_{\neg\phi}(w)$ の最小値を取れば良い．

また，$M_k \not\models \phi$ である時は，

$$A_{dist} \times A_{\neg\phi}(w'_k) = \infty$$

であるため，$A_{dist} \times A_{\neg\phi}(w)$ の最小値とはならない．

以上から Model Measuring を解くには，$A_{dist} \times A_{\neg\phi}$ に対する optimal-weight question を解けばよいことがわかる．