情報処理学会論文誌 Vol.53 No.2 548–556 (Feb. 2012)

# ソフトウェアモデル検査とテストケース生成の統合

橋本 祐介[1,2,a)] 中島 震[1,3]

受付日 2011年6月14日, 採録日 2011年11月7日

**概要**：有界モデル検査はプログラムの信頼性を向上させる有力な手段である．しかし，プログラムを有限状態遷移系へ変換する過程で，広い意味での近似を導入することから，誤警告や不具合の見過しを起こすという問題がある．本研究では，この問題に対して有界モデル検査をテストケース生成で補うツールを提案する．とくに，不具合の見過しの原因となる過小近似の場合について，有界モデル検査とテスト実行に共通のカバレッジ基準の下で，近似導入の有無を自動検知する方式を提案する．MINIX のソースコードを対象とした実験により，有界モデル検査とテスト実行とをあわせて，カバレッジ基準を満たす検査が行えることを示した．

**キーワード**：ソフトウェアモデル検査，モジュラ検証，近似，カバレッジ，テストケース生成

# Combining Software Model Checking and Test Case Generation

Yuusuke Hashimoto[1,2,a)] Shin Nakajima[1,3]

Received: June 14, 2011, Accepted: November 7, 2011

***Abstract:*** Bounded Model Checking (BMC) is a promising approach to achieving high quality of programs. In BMC, programs are translated into finite-state transition systems to introduce some approximation. It may result in false alarms or missing of errors. We propose a tool to augment BMC with test case generation. It includes an automated way of detecting under-approximation and a specification-based test case generation method, both of which employs a common coverage criteria. We also demonstrate the effectiveness of our approach by applying it to checking of MINIX source codes.

***Keywords:*** software model checking, modular verification, approximation, coverage, test case generation

## 1. はじめに

ソフトウェアの信頼性向上に関心が高まっている．従来からの信頼性向上手段であるテストは，プログラム実行によるので，テストケースごとに 1 つのパスしか検査せず，網羅度が低い．ロジック・モデル検査はすべてのパスを考慮した網羅探索を行う [10]．ソフトウェアモデル検査はモデル検査のプログラム自動検証への適用である．産業界では，信頼性の基準はテストで与えられており，自動検証ツールを使う場合であっても，テストによる検査との関係を論じる必要がある．

モデル検査には，状態爆発と呼ばれるスケーラビリティの問題があり，状態や状態遷移が大規模なプログラムについては，不具合の有無を判定できないことがある．状態数は，抽象化に基づく過大近似の導入により削減できる [9]．しかし，見かけのパスが増えることにより，実際には起こりえない不具合を検出するという誤警告の問題を起こす．有界モデル検査法 [6] は，探索範囲を一定の深さまでに限定し，不具合を効率良く検出する手法である．プログラム検証に適用する場合，対象プログラムを探索範囲内に制限する過小近似が必要となる．範囲外の不具合を見過す問題があるので，過小近似の導入には注意が必要である．

1 総合研究大学院大学
The Graduate University for Advanced Studies, Miura, Kanagawa 240–0193, Japan
2 日本電気株式会社サービスプラットフォーム研究所
Service Platforms Research Laboratories, NEC Corporation, Minato, Tokyo 108–8557, Japan
3 国立情報学研究所
National Institute of Informatics, Chiyoda, Tokyo 101–8430, Japan
a) yu-hash@cb.jp.nec.com

本研究では，有界モデル検査法を用いたモジュラ検証において，モデル検査における近似導入による問題をテストケース生成によって補うツールを提案する．提案方法では，モデル検査による警告が誤っていないことを，警告についての反例から生成したテストケースを実行して判定する．また，不具合の見過しの可能性を，モデル検査の方法を応用したトラップ挿入によって自動検知する．トラップはモデル検査とテストに共通のカバレッジ基準に則って挿入する．モデル検査をテストで補うことにより，近似の影響がなくなり，網羅度の高い検査ができる．実際，MINIXのソースコードを用いた実験により，モデル検査とテストとをあわせて，網羅度の高い検査が実施できた．

本稿は次の構成をとる．2 章では，本稿で用いる有界モデル検査ツールと，近似導入の問題について述べる．3 章では，モデル検査をテストケース生成で補うツールと手法を提案し，提案手法を MINIX の一部に適用した結果を 4 章に示す．5 章で関連研究に触れ，最後に，今後の課題を 6 章に述べる．

## 2. 背景

### 2.1 有界モデル検査ツール VARVEL

C プログラムの有界モデル検査ツールとして，CBMC [8]，F-Soft [17]，SMT-CBMC [3]，ESBMC [11] などがある．対象プログラムを有限状態遷移系として表す式を $C$，対象プログラムが満たすべき性質（プロパティ）を表す式を $P$ とすると，$C \Rightarrow P$ を示したい（$\Rightarrow$ は論理の含意）．有界モデル検査ツールは，前記論理式の否定である $C \wedge \neg P$ を満たす命題変数値の割当てを充足可能性判定器（SAT/SMT ソルバ）により探す．見つかった変数値の割当ては，対象プログラムがプロパティを満たさないことを示す反例，すなわち，ある初期状態からプロパティを満たさない状態に至るパスの一例である．見つからなければ，対象プログラムはプロパティを満足する．状態爆発により，指定時間内に探索が終わらない場合やメモリが不足する場合には，対象プログラムがプロパティを満たすかどうかは分からない．

本稿で用いる VARVEL は，F-Soft を基盤とする有界モデル検査ツールである [26]．逐次処理の C/C++プログラムを対象として，Design by Contract（DbC）に基づくモジュラ検証を行う．DbC は，事前・事後条件といった DbC 仕様をプログラムに明示して，堅牢なソフトウェアを構築する方法として提案された [21]．現在，DbC 仕様をプログラムのコメントとして追記する記法が提案されている [5], [18]．VARVEL は，独自の DbC 記法を提供し，次の (1)，(2) により，プログラム全体の検査を関数単位のモジュラ検証に分けて行う [15]．(1) 検査対象関数について，その事前条件を前提として，事後条件を満たすことを検査する．(2) 対象関数の関数呼び出しについては，呼ばれる関数のボディの代わりに DbC 仕様を用いて，その事前条件を満たして呼び出しが行われることを検査し，その事後条件を前提として呼び出し後を検査する．

具体的には，VARVEL は，コメント中の DbC 仕様をプリミティブ関数 $assert$ と $assume$ を用いたプログラムに変換する．プリミティブが評価される前の状態を $S$ とすると，$assert(C)$ は $S \Rightarrow C$ を検査すべきことを，$assume(C)$ は評価後の状態を $S \wedge C$ とすべきことを VARVEL に指示する．変換方法は関数の使い方の種類によって異なる．たとえば，コールツリーの起点となる関数であれば，事前条件 $Pre$ は $assume(Pre)$ として関数の開始箇所に，事後条件 $Post$ は $assert(Post)$ として終了箇所に挿入する．ソースコードを検査ツールに与えていない関数などについての変換方法は他の文献 [16] に示した．

さらに，VARVEL では関数ポインタを対象とした DbC 記法を提供する．また，関数ポインタを介した呼び出しに関する検査を，関数ポインタの仮 DbC 仕様を用いたモジュラ検証と，実際に呼ばれる各関数の DbC 仕様と仮 DbC 仕様との一貫性検査に分けて行う．関数ポインタの DbC 記法と検査方法について，MINIX を対象とした実験を行い，関数ポインタに関係する不具合を検出し，有効性を確認した [27]．

### 2.2 近似の問題

産業界では，信頼性の基準はテストで与えられており，たとえ自動検証ツールを使った場合であっても，テストによる検査との関係を論じる必要がある．

ソフトウェアモデル検査では，ロジック・モデル検査が適用できるように，対象プログラムを有限状態遷移系に変換する．モデル検査において，状態爆発というスケーラビリティの問題が起きると，有限状態空間上の探索を終えられず，不具合の有無を示せない．変換の際に抽象化といった過大近似を導入することにより，状態や状態遷移の数を減らして状態爆発を緩和できる [9]．しかし，過大近似によって見かけの振舞いが増える．逆に，過大近似されたプログラムは元のプログラムには存在しない見かけのパスを含む．プログラムが含むパスとその集合を $\pi$ と $\Pi$，変換の関数を $\alpha$ とし，変換後のプログラムにおけるパス・集合を $'$ で元のプログラムのそれと区別すると，過大近似は次のように表せる．

$$\forall \pi \in \Pi \cdot \exists \pi' \in \Pi' \cdot \pi' = \alpha(\pi).$$

$$\exists \pi' \in \Pi' \cdot \pi' \notin ran(\alpha) \quad (ran(\alpha) \text{ は } \alpha \text{ の値域})$$

見かけのパス上のみで検出される安全性の不具合は，元のプログラムでは起こりえない見かけの不具合である．見かけの不具合はバグの原因を調査する必要がないので，誤警告であることを自動判定したい．モデル検査の反例から不具合を再現しうるテストケースを生成する研究 [7] が判定に利用できる．

有界モデル検査法では，有限状態空間をある深さまでしか探索しないことにより，効率的に不具合を見つける．プログラムを探索範囲に制限するための工夫は，過小近似を導入することである．元のプログラムが変換後のプログラムの振舞いをすべて含むような近似を過小近似と呼ぶ．逆に，過小近似されたプログラムは元のプログラムの一部のパスを含まない．

$\forall \pi' \in \Pi' \cdot \exists \pi \in \Pi \cdot \pi' = \alpha(\pi)$.

$\exists \pi \in \Pi \cdot \pi \notin dom(\alpha)$ ($dom(\alpha)$ は $\alpha$ の定義域)

元のプログラムにしか存在しないパス上のみで起こる不具合は，変換後のプログラムを探索しても検出できない．不具合の見過しを防ぐためには，元のプログラムにおいてモデル検査では探索されないパスの有無を自動で検知したい．また，そのようなパスが検知されれば，モデル検査とは別の手段で検査したい．別手段としてはプログラムテストを考えることができる．

テストを行うには，テストケース（テスト入力と期待される結果）を生成するために，対象プログラムの仕様が必要となる．事前・事後条件といった仕様を同値分割などにより区分けし，区分ごとにテストケースを生成する研究がある [12], [19]．これを併用すればよい．

## 3. 統合ツール

### 3.1 近似の取扱いの方針

ソフトウェアモデル検査による検査結果は，近似導入の影響を受けている可能性がある．本研究では，ソフトウェアモデル検査とテストケース生成を組み合わせて，近似導入の自動判定やカバレッジ基準を満たす検査を行う方法を提案する．一般に，過大近似と過小近似は混在しうるため，あるパスにどの近似が導入されたかを特定することは難しい．そこで，パスがモデル検査により探索可能か，テストにより実行可能か，という観点から，近似導入の有無を調べる．

過大近似については，モデル検査で得られた反例からテストケースを生成し，テストによって不具合の再現を試みる．再現しなければ，不具合は過大近似の影響による見かけのものであり，反例は誤警告であると自動判定できる．

過小近似については，モデル検査の探索経路に存在すれば必ず反例が得られるトラップを対象プログラムに埋め込む．反例が得られなければ，トラップを含むパスはある箇所から探索されていない，すなわち，不具合の見過しの可能性を自動検知できる．検知した場合には，DbC 仕様からテストケースを生成し，テストを行う．テストと共通のカバレッジ基準に則って，検知用のトラップを埋め込むことにより，プログラムの大部分をモデル検査で網羅探索することを確認し，残りの部分を少ないテストケースで補助的に検査するといった，従来のテストのみによる方法に比べて網羅度の高い検査ができる．

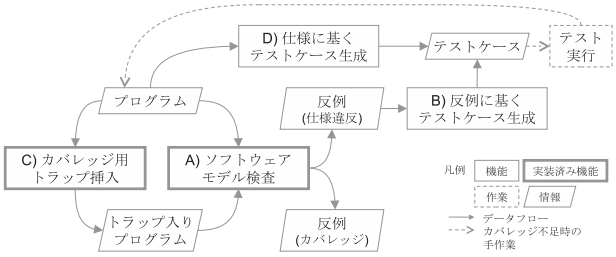


図 1 ツールの概要
**Fig. 1** Overview of a proposed tool.

```
    doSWMCandTest( program )
1     result1 := doSWMC( program );
2     if ( swmcFailed( result1 ) )
3     then doTCGfromSpec( program );
4     else
        /* for Over-Approximation */
5       foreach counterexample in result1
6         doTCGfromCE( counterexample, program );
        endloop
        /* for Under-Approximation */
7       trapProgram := instrumentTrap( program );
8       result2 := doSWMC( trapProgram );
9       uncovered := false
10      foreach trap in trapProgram
11        if ( notFoundCounterExample( trap, result2 ) )
12        then uncovered := true;
          endif
        endloop
13      if ( uncovered )
14      then doTCGfromSpec( program );
        endif
      endif
```

図 2 有界モデル検査をテストケース生成で補うアルゴリズム
**Fig. 2** Algorithm to enhance BMC with TCG.

### 3.2 ツールの概要

本稿で提案する，有界モデル検査とテストケース生成を統合するツールの概要を図 1 に示す．このツールは，検査の対象プログラムについて有界モデル検査を行うソフトウェアモデル検査機能 A，有界モデル検査で得られた反例からテストケースを生成する反例に基づくテストケース生成機能 B，対象プログラムに過小近似の検知用のトラップを挿入するカバレッジ用トラップ挿入機能 C，対象プログラムの DbC 仕様からテストケースを生成する仕様に基づくテストケース生成機能 D，の 4 つの機能からなる．本稿の時点では，機能 A と C を実装している．機能 B と D はそれぞれ既存研究 [7] と [19] をもとに実装可能である．

ツールが行う処理のアルゴリズム doSWMCandTest を図 2 に示す．doSWMCandTest は，機能 A によって，ソフトウェアモデル検査を行う（行 1）．指定時間内に探索が終わらな

```
    #define  SIZ  1024
1   extern int a[SIZ];
2   extern int g;
3   /** @invariant g==-1 || g==0 */
4   /** @post  __return==0 || __return==1 */
5   int bar();
6   /** @pre __exist( k, 0, SIZ-1, a[k]==v ) ||
            __foreach( k, 0, SIZ-1, a[k]!=v )
7       @post 0<=__return && a[ __return ]==v || __return==-1
     */
8   int foo( int v ){
9     int r=-1, i=0;
10    if ( bar()+g==1 ) {
11      r=-2; /* BUG */
12      while ( i<SIZ ) {
13        if ( v==a[i] ) { r=i; break; }
14        i=i+1;
        }
      }
15    return r;
    }
```

**図 3** 過小近似の影響を受けるプログラム例
**Fig. 3** Example with a loop.

い場合は，機能 D によって，DbC 仕様からテストケースを生成し，終了する（行 2，3）．モデル検査の結果が仕様違反の反例を含む場合，機能 B によって，反例に基づいてテストケースを生成する（行 4–6）．生成されたテストケースを実行して，不具合が再現しなければ，反例は過大近似による誤警告であることが分かる．過小近似への対応としては，まず，機能 C によって，カバレッジ基準に則って決めた箇所が探索された場合に真になるトラップ変数と，トラップ変数が偽であるというトラップ表明とを，対象プログラムに挿入する．次に，機能 A によって，トラップ入りプログラムに対してモデル検査を行いトラップ表明違反の反例を得る（行 7，8）．この反例は，トラップ変数が真になること，すなわちカバレッジ基準に則って決めた箇所をモデル検査によって探索したことを示す．最後に，1 つでも反例の無いトラップ表明があれば，未探索箇所があるものとして，機能 D によって，DbC 仕様からテストケースを生成し，終了する（行 9–14）．なお，生成されたテストケースを用いて反例のないトラップの箇所を実行できない場合には，DbC 仕様をさらに詳細に場合分けしてテストケースを生成し直す必要がある．

モデル検査の反例からテストケースを生成することはよく知られており，反例の初期状態において変数に割り当てられた値をテスト入力とする [2]．以降の 3.3，3.4 節では，モデル検査では探索されない箇所の検知と DbC 仕様からのテストケース生成について述べる．

### 3.3 近似導入の検知方法

過小近似の導入による問題について，ループの繰返しを所与の回数に限定する近似を例として，**図 3** を用いて説明する．プログラムの複雑さに応じて状態遷移は様々に変わるので，有界モデル検査の探索の深さとループの繰返し回数の上限との関係は一意には決まらない．ここでは，簡単のため所与の回数を 2 回とする．検査の対象関数 `foo` の DbC 仕様では，引数 `v` は，大域配列 `a` のいずれかの要素と値が同じか，すべての要素と値が異なる（行 6）．`foo` の戻り値は `0` 以上か`-1` であり，前者の場合は戻り値を添え字とする `a` の要素が `v` と同じ値を持つ（行 7）．`foo` の関数ボディでは，他の関数 `bar` の戻り値と大域変数 `g` の値の和が `1` の場合に（行 10），`while` ループ内で，配列 `a` の各要素を調べ，引数 `v` と値の同じ要素があれば，その要素の添え字を返し（行 12–14，15），それ以外の場合には，本来は`-1`（行 9，15）を返す．図 3 では変数 `r` に`-2` が代入されることがあり（行 11），そのまま `r` が戻り値として使われると，事後条件への違反となる．過小近似されたプログラムは，ループボディ（行 13，14）の 3 回目の実行を行う前に処理を終了する．このプログラムをモデル検査で検証すると，事後条件違反の不具合は検出されない．しかし，ループボディの 3 回目以降については，モデル検査では調べておらず，事後条件が守られたのかどうかは分からない．

プログラムのパスは無数にありうるので，探索されないパスを探し尽くすことは難しい．パスの代わりに，プログラムの特定の箇所が探索されないことを検知する．この検知は，特定の箇所でのみ真になるトラップ変数を埋め込み，対象プログラムの終了箇所でトラップ変数が偽であるというプロパティをモデル検査で調べればよい．反例がなければ，特定の箇所は探索されていない．探索されない箇所というプログラム内部の性質について調べるので，プログラム構造に着目したカバレッジ基準に則って，特定の箇所を決める．カバレッジ基準としては，CACC（Correlated Active Clause Coverage）[1] を用いる．CACC は産業界で実用的に使われている masking MCDC に相当する．分岐文やループ文における制御式の全体を述語と呼ぶ．述語は二項論理演算子（∨，∧）で結合された節からなり，節は二項論理演算子を含まない．着目した 1 つの節を主節と呼び，残りの節を副節と呼ぶ．ある述語についてのテストが CACC を満たすためには，その述語の任意の主節について次の 2 点が要求される．[TR1] 主節は真と偽のいずれにも評価されることがある．[TR2] 主節のある値について述語を真にするような副節の値の組があり，主節のもう一方の値について述語を偽にするような副節の値の組がある．なお，TR2 において副節の値の組は異なっていてもよい．

カバレッジ基準に則ったトラップを埋め込むために，**表 1** の整形ルールを用いて，プログラムを整形し，トラップ入りプログラムを得る．表 1 にはないが，ループ文（`for`，`do`），分岐文（`switch`），論理演算子（`!`，`||`）といった他の言語要素についても同様のルールを決められる．

整形では，まず，ルール aN（N = 1,···）によって，制御

表 1 トラップ挿入のための整形ルール（一部）
**Table 1** Some transformation rules to insert traps.

| | | |
|---|---|---|
| a1 | | `while (P) { S }` （p は定数を除く） |
| | → | `while (1) { if (P) { ; } else { break; } S }` |
| a2 | | `if (P) { S }` （P は `pred` を除く） |
| | → | `if (P) { pred=1; } else { pred=0; } if (pred) { S }` |
| b1 | | `if ( P && Q ) { pred=b1; S } else { pred=b2; T }` |
| | → | `if ( P ) { if ( Q ) { pred=b1; S } else { pred=b2; T } }` |
| | | `else { pred=b2; T }` |
| c1 | | `if (P) { pred=b; }` → `if (P) { pred=b; trap_i_j=1; }` |
| c2 | | `else { pred=b; }` → `else { pred=b; trap_i_j=1; }` |
| d | | `return <戻り値>;` |
| | → | `__assert(trap_i_j==0);` （トラップ変数分，繰り返す） |
| | | `return <戻り値>;` |

→：左辺と右辺はそれぞれ整形前と後．`b,b1,b2`：真偽値（`b1≠b2`）．`&&`：論理積．`!`：否定．
`P,Q`：述語．`S,T`：空ではない文やブロックの並び．`pred`：述語の値を保持する変数．
`trap_i_j`：トラップ変数，i は関数ごとの述語の連番，j は述語ごとの節の組合せの連番．

式（述語）の値を保持する変数 `pred` を導入し，元のループや分岐全体を，`pred` に値を代入する文の集まりと，`pred` の値に応じて元のループボディや副文を行う文の集まりに分ける．以降の変換は，`pred` に値を代入する文の集まりに対して行う．次に，ルール b1 によって，`pred` に真偽値を代入する分岐を，述語を節に分解した入れ子の分岐に変換する．変換後の分岐全体において，ある分岐に着目すると，その分岐の節の値によって，述語 `pred` に異なる真偽値（表 1 の b1，b2）を代入する文を持つ末端のブロックが存在するので，CACC の要求 TR1 を満たしうる．また，そのようなブロックへのパスを考えると，他の節の値の組を決めることができるので，CACC の要求 TR2 を満たしうる．すなわち，モデル検査によって末端のブロックをすべて探索すれば，CACC を満たす検査を行えたといえる．その後，ルール cN（N = 1,...）によって，分岐の末端のブロックにトラップ変数 `trap_i_j`（i = 1,···. j = 1,···）を導入し，ブロックが探索されたことを示す値として真（`1`）を代入する（トラップ変数は偽（`0`）で初期化する）．最後に，ルール d によって，`return` 文の直前に，トラップ変数ごとに，その値が偽であるというトラップ表明 `__assert(trap_i_j==0);` を挿入する．モデル検査によって見つかったトラップ表明違反の反例は，トラップ変数に真を代入する箇所が探索されたことを示す．トラップ表明のすべてについて反例が見つかれば，CACC を満たす探索が行われており，1 つでも反例が見つからなければ，探索されない箇所があることが検知されたと結論づけてよい．

**図 4** は，図 3 のプログラムを，表 1 のルールを用いて整形した例である．図 3 の行 10 と 13 の `if` 文および行 12 の `while` 文は，それぞれ図 4 の行 10a–c と 13a–c および 12a–d に整形される．トラップ入りプログラム（図 4）に対するモデル検査のカバレッジを**表 2** に示す．見出し行の「i, j」はトラップ変数 `trap_i_j` に対応しており，SWMC

```
 8  int foo( int v ){
 9    int r=-1, i=0;
10a   if ( bar()+g==1 )  { pred=1; trap_1_1=1; }
10b   else               { pred=0; trap_1_2=1; }
10c   if ( pred ) {
11      r=-2; /* BUG */
12a     while ( 1 ) {
12b       if ( i<SIZ )   { pred=1; trap_2_1=1; }
12c       else           { pred=0; trap_2_2=1; }
12d       if ( pred ) { ; } else { break; }
13a       if ( v==a[i] ) { pred=1; trap_3_1=1; }
13b       else           { pred=0; trap_3_2=1; }
13c       if ( pred ) { r=i; break; }
14        i=i+1;
        }
      }
15a   __assert( trap_1_1==0 );  __assert( trap_1_2==0 );
15b   __assert( trap_2_1==0 );  __assert( trap_2_2==0 );
15c   __assert( trap_3_1==0 );  __assert( trap_3_2==0 );
15    return r;
    }
```

**図 4** 未探箇所を検知するためのトラップ入りプログラムの例
**Fig. 4** Example with inserted traps.

表 2 モデル検査とテストによるカバレッジの例
**Table 2** Example of coverage by model checking and testing.

| | 1,1 | 1,2 | 2,1 | 2,2 | 3,1 | 3,2 |
|---|---|---|---|---|---|---|
| SWMC | Y | Y | Y | | Y | Y |
| Test | Y | Y | Y | Y | Y | Y |

見出し i, j：i 番目の述語における節の値の j 番目の組合せ

行の各セルの Y はトラップ変数に真（`1`）を代入する箇所がモデル検査で探索されたことを示す．ループボディを 2 回のみ実行する近似の導入により，`while` 文の制御式 `i<SIZ` が偽となる場合（図 4 行 12c）が探索されていないことが分かる．

```
1  int bar() { return 1; }  /* Ql */
2  void test1(){
3    int result, defining;
4    a[0]=999, …;           /* Random */
5    int v=999;             /* Pi ∧ Gj */
6    g=0;                   /* Ik */
7    result = foo(v);
8    defining = (0<=result && a[result]==v); /* Dj */
9    if (defining) printf("OK"); else printf("NG");
   }
```

図 5 テストプログラムの例
**Fig. 5** Example test program.

### 3.4 DbC 仕様からのテストケース生成

ソフトウェアモデル検査で探索されない箇所が見つかった場合，DbC 仕様からテストケースを生成し，テストを行う．検査対象の関数について，その事前条件 $Pre$ と事後条件 $Post$ は，次の DNF 形式であるとする．任意の論理式は DNF 形式に変換可能なので一般性を失わない．

$$Pre = \bigvee_i P_i, \quad Post = \bigvee_j Q_j = \bigvee_j (G_j \wedge D_j)$$
(各 $P_i$ は互いに素．$Q_j$ も同様)

各事後条件 $Q_j$ はガード条件 $G_j$ と定義条件 $D_j$ から構成されており，ガード条件は関数によって値が変更される変数を含まず，定義条件はそれらを含む．関数全体の振舞いは機能シナリオフォーム $FSF$ で表される．

$$FSF = \bigvee_{i,j} fs_{ij} = \bigvee_{i,j} (P_i \wedge G_j \wedge D_j)$$

$FSF$ 中の各 $fs_{ij}$ を機能シナリオと呼ぶ．上記 $FSF$ は，Liu らが提案した $FSF$ [19] に対して，事前条件も DNF 形式とし，機能シナリオをより細分化してある．テストケース生成では，対象関数の機能シナリオ以外に，対象関数によって参照・更新される大域変数の値域や，対象関数から呼ばれる関数の振舞いも考慮する必要がある．たとえば，図 3 のプログラム例では，行 10 の `if` 文の制御式 `bar()+g==1` が真および偽となるような大域変数 `g` の値と関数 `bar` の戻り値の組合せをテストする必要がある．そこで，大域変数の不変条件 $Inv = \bigvee_k I_k$ と呼ばれる関数の事後条件 $Post^{called} = \bigvee_l Q_l$ も考慮して，$P_i \wedge G_j \wedge I_k \wedge Q_l$ を満足する変数値を求めて，テスト入力・呼ばれる関数の戻り値・大域変数の事後の値とし，$D_j$ を期待結果とする．図 3 のプログラム例では，対象関数の事前条件は，`__exist(k, 0, SIZ-1, a[k]==v)` と `__foreach(k, 0, SIZ-1, a[k]!=v)` の 2 通り，大域変数の不変条件は，`g==-1` と `g==0` の 2 通り，呼ばれる関数の事後条件も `bar` の戻り値`==0` と `bar` の戻り値`==1` の 2 通りで，合計 8 通りの組合せがある．

図 3 のプログラム例に対して，DbC 仕様をもとに生成したテストプログラムを**図 5** に示す．関数 `bar` については事後条件`__return==1` を満たすスタブ関数を生成する（行 1）．機能シナリオに出現しない大域配列 `a` の各要素の値はランダムに生成する（行 4）．検査対象の引数と大域変数には，それぞれ $P_i \wedge G_j$ と $I_k$ を満たす値を充足可能性判定ソルバを用いて求める（行 5，6）．テストプログラムは，生成したテスト入力を与えて対象プログラムを実行し（行 7），実行結果について定義条件の値を調べ，ログを出力する（行 8，9）．元のプログラムの代わりに，トラップ入りプログラム（図 4）を用いて，トラップ変数の値を調べる`__assert` のログ出力に置き換えてカバレッジを調べた結果を表 2 の Test 行に記す．ソフトウェアモデル検査をテストで補完することにより，両者をあわせて少なくとも CACC 以上の網羅度での検査が行えている．

## 4. 実験と考察

提案ツール（図 1）において，トラップ挿入ツールを作成し，既存のソフトウェアモデル検査ツール VARVEL と組み合わせて，オープンソースの OS である MINIX（Version 3.1.1）のソースコードの一部に適用した．MINIX は，ソースコードが公開されている点と，文献 [25] に仕様が記載されている点で，DbC の検査を行いやすい．MINIX は，マイクロカーネルアーキテクチャを採用しており，サーバ，カーネル，ドライバ層の各プロセス間でのメッセージ通信による協調動作を特徴とする．ユーザアプリケーションからドライバへの要求は，サーバ層のファイルシステム機能を介して行われる．とくにファイルシステム機能のファイル `device.c` にはドライバとのメッセージ通信に関する関数が集められており，文献記載の MINIX の特徴を検査するのに適している．

`device.c` の主要な関数について，本稿の提案手法に則って，ソフトウェアモデル検査を行い，探索されない箇所があればテストケースを生成して，テストを行った．その結果を**表 3** に示す．DbC 仕様としては，メッセージのタイプは特定の整数値であること，プロセス番号は –4 以上かつ 100 未満であること，デバイス番号は 0 であるか，16 ビット中の上位 8 ビットが 32 未満であること，処理の結果を表す値は成功が 0 であり，失敗が負値であること，の 4 点を DNF 形式で記述した．モデル検査では，これらの DbC 仕様をプロパティとした．テストケースは，DNF 形式の DbC 仕様の各節から引数や大域変数の代表値の組を求め，これらの代表値の組の直積として得た．各代表値は充足可能性判定ソルバ Yices [13] を用いて線形演算の範囲で求めた．

表 3 の関数 `dev_open` では，6 個のトラップのすべてをモデル検査で探索できたので，テストは実行していない．列#Test と#TC の`--`は，テストケース生成およびテスト実行を行わなかったことを示す．関数 `dev_status` では，21 個のトラップのうち 19 個をモデル検査によって探索した．また，残りの 2 個のトラップを含む 4 個のトラップを

表 3 MINIX への提案手法の適用結果
**Table 3** Result of applying proposed approach to MINIX.

| Function | Size | #Trap | #BMC | #Test | #Total | #TC |
|---|---|---|---|---|---|---|
| dev_open | 20 | 6 | 6 | – | 6 | – |
| dev_close | 9 | 2 | 2 | – | 2 | – |
| dev_status | 41 | 21 | 19 | 4 | 21 | 1 |
| dev_io | 48 | 8 | 8 | – | 8 | – |
| tty_opcl | 32 | 9 | 4 | 8 | 9 | 32 |
| ctty_opcl | 12 | 2 | 2 | – | 2 | – |
| do_setsid | 16 | 2 | 2 | – | 2 | – |
| do_ioctl | 39 | 5 | 5 | – | 5 | – |
| gen_io | 76 | 25 | 22 | 18 | 25 | 144 |
| ctty_io | 21 | 2 | 2 | – | 2 | – |
| clone_opcl | 52 | 7 | 7 | – | 7 | – |

Function：関数名．Size：関数の空白行を除く行数．#Trap：カバレッジ測定用のトラップ変数の個数．
#BMC：有界モデル検査（BMC）で探索されたトラップの個数．
#Test：テストで実行されたトラップの個数．
#Total：BMC とテストのいずれかでカバーされたトラップの個数．
#TC：生成されたテストケースの個数．

表 4 MINIX を対象としたモデル検査とテストによるカバレッジ
**Table 4** Coverage in MINIX by model checking and testing.

| | 1,1 | 1,2 | 2,1 | 2,2 | 2,3 | 3,1 | 3,2 | 4,1 | 4,2 | 5,1 | 5,2 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SWMC | | Y | Y | Y | Y | | Y | Y | Y | Y | Y |
| Test | Y | Y | | Y | | Y | | | | | |

| | 6,1 | 6,2 | 7,1 | 7,2 | 8,1 | 8,2 | 8,3 | 8,4 | 9,1 | 9,2 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SWMC | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | |
| Test | | | | | | | | | | | |

見出しの i，j：i 番目の述語における節の値の j 番目の組合せ

1 個のテストケースによって実行した．dev_status の各トラップが有界モデルとテスト実行により，どのようにカバーされたかを**表 4** に示す．見出し行の i,j はトラップ変数 trap_i_j に対応する．SWMC 行の Y はトラップがソフトウェアモデル検査によって探索されたことを，Test 行の Y はテスト実行されたことを示す．列 1,1 と 3,1 を見ると，ソフトウェアモデル検査をテスト実行で補えたことが分かる．

テストケースが十分ではなく，実行できないトラップがある場合には，プログラムコードを調べて，トラップに関係する DbC 仕様をより詳しく記述し，テストケースを作り直した．たとえば，関数 gen_io では，呼ばれる関数_sendrec の戻り値が 0 以下であるという事後条件 (__return<=0) を，戻り値の値を明示した DNF の式 (__return==0 || __return==-101 || ···) に修正した．テストケースの作り直しは，gen_io では，戻り値の場合分けが多く，人手の作業に約 1 時間かかったが，tty_opcl では約 10 分であった．修正後の DbC 仕様を用いても，表 3 のモデル検査で探索したトラップの数は変わらなかった．

表 3 では，全トラップ 89 個のうち，89%にあたる 79 個のトラップが有界モデル検査によって探索された，すなわち，各トラップについて，トラップ変数に真を代入する箇所を通って関数の終了箇所に至るパスが網羅探索された．対象プログラムの大部分を有界モデル検査によって網羅的に検査し，残りの一部についても分岐カバレッジ基準 CACC を満たすテストを行っており，従来のテストのみの検査に比べてカバレッジの高い検査を実施できた．

引数や大域変数の値域の直積としてテストケースを生成する方法を用いて，テストのみで CACC 基準を満たそうとすると，関数 gen_io の場合，9,418 個のテストケースが必要であった．変数値の組合せを特定するように DbC 仕様を記述し，テストケースを減らすことができるが，プログラムの内部構造にあわせて DbC 仕様を場合分けする必要があり手間がかかる．できるだけ多くの範囲を有界モデル検査で網羅的に検査し，一部についてのみテストケースを考慮する本稿のアプローチはテストの省力化という点で有効な方法である．

## 5. 関連研究

有界モデル検査法を用いてプログラムを検査するツール [3], [8], [11], [17], [26] は不具合の検出に有効である．有界モデル検査を適用するために，プログラムを有限状態遷移系に変換する際に，近似を導入することがある．ループを固定回数分のループボディの繰返しとするような変換を行うと [8]，有界モデル検査では固定回数を超える部分を含むパスを探索しない．そのようなパス上の不具合は見過ごされる．探索の深さに制限されないように有界モデル検査を拡張する手法 [20], [23] が提案されているが，本稿ではテストとの役割分担という方法を提案した．産業界では，信頼性の基準はテストで与えられており，たとえ自動検証ツールを使った場合であっても，テストによる検査との関係を論じる必要があることが理由である．

モデル検査では，対象を有限状態遷移系として表現する必要がある．対象の設計を自動的にモデル検査用の表現に変換する研究がある [22]．状態遷移図の情報を，実行の意味が厳密な同期型言語に変換し，さらにモデル検査器ごとの表現に変換することにより，様々なモデル検査器に対応する．プログラムの自動検証でも，プログラムを中間言語に変換することにより，様々な定理証明器に対応する研究がある [14]．本稿の方式は，モデル検査を行うだけでなく，モデル検査の誤警告やカバレッジ不足の問題について，その原因である近似の導入を検知し，テストケースを生成する点で，これらの研究と異なる．プログラムを有限状態遷移系に自動変換する既存のソフトウェアモデル検査ツールを用いるため，中間言語は必要としない．近似の検知を，反例に基づくテストケース生成や，プログラミング言語の段階でのプリミティブ（*assert*，*assume*）を用いたトラッ

プ挿入といった汎用的な方法で行うので，様々なソフトウェアモデル検査ツール [8], [17], [24] に対応可能な方式である．

単体テストが十分であるかはプログラム構造に関するカバレッジで測る．本稿では，分岐カバレッジ基準として CACC [1] を採用し，モデル検査のカバレッジを測る．検査対象にトラップ変数を挿入して，意図したパスを示す反例をモデル検査によって得る考え方がある [7]．本稿では，分岐の述語を節に分解し，節の真偽の組合せごとにトラップを挿入することにより，モデル検査が CACC を満たすパスを探索したことを調べる．

しかし，有限状態空間を網羅探索するモデル検査のカバレッジを，CACC のような分岐カバレッジ基準で測ることは適切とはいい難い．パスカバレッジはパスが無数にありうるため，カバレッジ基準としては不適切である．関連研究として，PCT（Predicate Complete Testing）カバレッジ [4] が提案されている．対象プログラムの文の個数 $M$ と述語の個数 $n$ に対して，各文における述語のとりうる値の組を 1 つの状態とする．対象プログラムをブーリアンプログラムに変換し，ブーリアンプログラム上のパスをたどって各状態への到達性を調べて，到達可能な状態の総数をカバレッジの分母とする．状態の総数は最大でも $M \times 2^n$ なので，分母を有限におさえることができる．モデル検査のカバレッジは，PCT カバレッジのようにパスを考慮し，かつ母数が有限のカバレッジ基準を用いて測ることが望ましい．

## 6. おわりに

有界モデル検査法を用いたソフトウェアモデル検査において，過小近似によって探索されない箇所が生じるという問題を明らかにし，探索されない箇所の検知と DbC 仕様からのテストケース生成とをあわせて，ソフトウェアモデル検査を補完する手法を提案した．また，探索されない箇所の検知を自動化して，MIINX の一部のソースコードに提案手法を適用する実験を行い，提案手法の有効性を確認した．本稿では，VARVEL を具体的な有界モデル検査ツールとして，提案方法の考察・実験を行った．しかし，提案方法は，CBMC など C プログラムの有界モデル検査ツール一般に適用可能である．

今後の課題については，より大規模な実験が必要である．

また，カバレッジ基準については，PCT カバレッジのようなモデル検査の特性を考慮した基準が好ましく，検討の余地がある．

さらに，ツール全体の実装といった技術面の課題に加えて，DbC 仕様の書き方についての課題もある．ロジック・モデル検査では，調べたい性質を時相論理式で表現する．すべてのパス上のすべての状態や，あるパス上の状態 1 に続く状態 2 といった，パスおよび時間にまたがる多様な表現が可能である．一方，モジュラ検証における DbC 仕様は，プログラムの特定の箇所で取得できる変数値を用いた局所的な条件である．時相論理における表現の一部分しか，あるいはまったく，表現できないことがある．また，DbC 仕様の詳細度には，検査の精度とモデル検査の探索の性能に関するトレードオフがある．入力や出力の値域を記すにとどめると，粗い検査しかできないが，探索は早い．入力と出力の対応関係を細かく場合分けして記すと，探索は遅いが，木目細かい検査ができる．しかし，どこまで詳しく DbC 仕様を記すべきかは自明ではない．実用化に向けては，これらの課題に対して，DbC 仕様として記述できる・できない性質についての情報を提供し，プログラムの仕様をどこまで詳しく記述するかなどのノウハウを蓄積する必要がある．

### 参考文献


[1] Ammann, P. and Offutt, J.: *Introduction to Software Testing*, Cambridge University Press (2008).

[2] Ammann, P.E., Black, P.E. and Majurski, W.: Using Model Checking to Generate Tests from Specifications, *Proc. ICFEM*, pp.46–54, IEEE Computer Society (1998).

[3] Armando, A., Mantovani, J. and Platania, L.: Bounded Model Checking of Software using SMT Solvers instead of SAT Solvers, *Proc. SPIN*, pp.146–162 (2006).

[4] Ball, T.: A Theory of Predicate-Complete Test Coverage and Generation, Technical Report, Microsoft Research Technical Report, MSR-TR-2004-28 (2004).

[5] Baudin, P., Filliâtre, J.-C., Marché, C., Monate, B., Moy, Y. and Prevosto, V.: ACSL: ANSI/ISO C Specification Language (2008).

[6] Biere, A., Cimatti, A., Clarke, E.M. and Zhu, Y.: Symbolic Model Checking without BDDs, *Proc. TACAS*, pp.193–207 (1999).

[7] Callahan, J., Schneider, F. and Easterbrook, S.: Automated Software Testing Using Model-Checking, *Proc. SPIN* (1996).

[8] Clarke, E., Kroening, D. and Lerda, F.: A Tool for Checking ANSI-C Programs, *Proc. TACAS*, pp.168–176 (2004).

[9] Clarke, E.M., Grumberg, O. and Long, D.E.: Model Checking and Abstraction, *ACM TOPLAS*, Vol.16, No.5, pp.1512–1542 (1994).

[10] Clarke, E.M., Grumberg, O. and Peled, D.A.: *Model Checking*, The MIT Press (1999).

[11] Cordeiro, L., Fischer, B. and Marques-Silva, J.: SMT-Based Bounded Model Checking for Embedded ANSI-C Software, *Proc. ASE*, pp.137–148 (2009).

[12] Dick, J. and Faivre, A.: Automating the Generation and Sequencing of Test Cases from Model-Based Specifications, *Proc. FME*, pp.268–284 (1993).

[13] Dutertre, B. and Moura, L.D.: A Fast Linear-Arithmetic Solver for DPLL(T), *Proc. CAV*, pp.81–94, Springer (2006).

[14] Filliâtre, J.-C. and Marché, C.: Multi-prover Verification of C Programs, *Proc. ICFEM*, pp.15–29 (2004).

[15] Hashimoto, Y. and Nakajima, S.: Modular Checking of C Programs Using SAT-Based Bounded Model Checker, *Proc. APSEC*, pp.515–522 (2009).

[16] Hashimoto, Y. and Nakajima, S.: Modular Checking with Model Checking, *Proc. SSV*, pp.105–122 (2009).
[17] Ivančić, F., Shlyakhter, I., Gupta, A., Ganai, M.K., Kahlon, V., Wang, C. and Yang, Z.: Model Checking C Programs Using F-Soft, *Proc. ICCD*, pp.297–308 (2005).
[18] Leavens, G.T., Poll, E., Clifton, C., Cheon, Y., Ruby, C., Cok, D., Müller, P., Kiniry, J., Chalin, P. and Zimmerman, D.M.: JML Reference Manual (2008).
[19] Liu, S. and Nakajima, S.: A Decompositional Approach to Automatic Test Case Generation Based on Formal Specifications, *Proc. SSIRI*, pp.147–155 (2010).
[20] McMillan, K.L.: Interpolation and SAT-based Model Checking, *Proc. CAV*, pp.1–13 (2003).
[21] Meyer, B.: Applying Design by Contract, *IEEE Computer*, Vol.25, No.10, pp.40–51 (1992).
[22] Miller, S.P., Whalen, M.W. and Cofer, D.D.: Software Model Checking Takes Off, *Comm. ACM*, Vol.53, pp.58–64 (2010).
[23] Moura, L.D., Ruess, H. and Sorea, M.: Bounded Model Checking and Induction: From Refutation to Verification, *Proc. CAV*, pp.14–26 (2003).
[24] Rodriguez, R.E., Dwyer, M. and Hatcliff, J.: Checking Strong Specifications Using An Extensible Software Model Checking Framework, *Proc. TACAS*, pp.404–420 (2004).
[25] Tanenbaum, A.S.：オペレーティングシステム第3版，ピアソンエデュケーション (2007).
[26] 宮崎義昭，橋本祐介：C言語へのフォーマルメソッドの適用，情報処理，Vol.49, No.5, pp.514–520 (2008).
[27] 橋本祐介，中島 震：有界モデル検査法を用いたCプログラムのモジュラー検証，情報処理学会論文誌，Vol.52, No.8, pp.2422–2430 (2011).

**橋本 祐介** （学生会員）

1989年東京大学大学院理学系研究科修士課程修了．同年日本電気株式会社入社（現在に至る）．2008年総合研究大学院大学複合科学研究科情報学専攻博士後期課程．

**中島 震** （正会員）

1981年東京大学大学院理学系研究科修士課程修了．NEC，法政大学を経て，2004年情報・システム研究機構国立情報学研究所教授．2005年総合研究大学院大学教授（併任）．この間，1988～89年米国オレゴン大学客員研究員，2001～07年科学技術振興機構PRESTOおよびSORST研究員（兼務），2004～07年北陸先端科学技術大学院大学JJREX客員教授．学術博士（東京大学）．2002年度山下記念研究賞，2003年度日本ソフトウェア科学会論文賞受賞．ディペンダブルソフトウェア工学，形式手法，モデル検査，モデリングに関する研究に従事．日本ソフトウェア科学会，ACM各会員．