様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月　 ４ 日現在

機関番号：１２６０８
研究種目：若手研究(B)
研究期間：2012～2014
課題番号：２４７０００２６

研究課題名（和文）割込み処理に伴う競合の高精度かつ高効率な検出手法に関する研究

研究課題名（英文）Study of Highly Accurate and Efficient Int-Race Detection

研究代表者
荒堀　喜貴（Arahori, Yoshitaka）

東京工業大学・情報理工学（系）研究科・助教

研究者番号：５０６１３４６０

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：本研究は，割込み処理を用いるソフトウェアの信頼性及び開発効率の向上のために，割込み処理に起因する競合（割込み競合）を高精度かつ高効率に検出する手法の実現を目的としていた．主な研究成果として，（1）多重割込みの可能性も考慮し従来より多くの割込み競合を正確に検出する方式，（2）少ない空間使用量で多数の検出を可能にするメタデータ管理方式，（3）複数の競合解析を並列実行可能なアルゴリズムを設計し実装した．

研究成果の概要（英文）：Our research goal was to improve the reliability and development efficiency of interrupt-driven software by realizing a highly accurate and efficient detector for int-races, i.e., data races caused by interrupt handling. To achieve this goal, we have designed and implemented (1) a precise detection scheme which can find more int-races including those incurred by multiple interrupts, (2) the efficient metadata management which enables the accurate int-race detection with low memory overhead, and (3) an efficient algorithm which can concurrently detect multiple int-races.

研究分野：情報科学

キーワード：プログラム解析　バグ検出　割込み　スレッド　競合

１．研究開始当初の背景

プログラムの信頼性や開発効率の低下の原因として悪名高いバグの１つに競合状態がある．このうちスレッド処理に伴う競合状態（以降，スレッド競合と呼ぶ）の検出手法は現在まで活発に研究されており，高精度な手法や高効率な手法が比較的多数存在する．

一方，割込み処理に伴う競合状態（以降，割込み競合と呼ぶ）の検出手法は研究例が非常に少なく，かつ，既存手法には精度や効率の面で大きな問題点がある．

組込みソフトウェアやネットワークプログラム等は割込み処理を多用するため，割込み競合の検出手法が十分に研究されていないことはそれらの信頼性や開発効率に大きな悪影響を及ぼす可能性がある．このため，精度や効率に優れる割込み競合検出手法が求められていた．

２．研究の目的

本研究では，割込み処理を行うプログラムの信頼性及び開発効率の向上に貢献するために，割込み処理に伴う競合状態を高精度かつ高効率に検出する手法を提案，実現することを目的とした．

３．研究の方法

上記研究目的の達成に向けて，以下の方法で研究を行った．

（1）各種のスレッド競合の検出手法から割込み競合の検出手法への拡張
（2）割込み競合の検出に向けて拡張した各種の解析手法の特性分析
（3）割込み競合検出手法の高精度化または高効率化に有効な解析手法の特定及び実現

４．研究成果

上記の方法に沿って研究を行い，以下の成果を得た．

（1）各種のスレッド競合検出手法の拡張に基づく割込み競合検出手法の実現

割込み競合検出法の実現方針として，既存のスレッド競合検出法を割込み競合の検出が可能となるように拡張した．

平成 24 年度の前半は，拡張の準備として，精度・効率面で多様な特性を持つ 4 種類のスレッド競合検出手法(happens-before 解析，ハイブリッド解析，サンプリング，静的解析との併用)を対象として文献調査を行い，各々のスレッド競合検出法をオープンソースのコンパイラ基盤（GCC）上に実装した．POSIX スレッドライブラリを利用する C プログラムのスレッド競合の検査が可能となるよう，GCC のコンパイラの最適化パスを改変して対象プログラムのコンパイル時に競合検査コードを挿入できるようにするとともに，競合検査を担う実行時検査ライブラリを実装した．

平成 24 年度の後半は，前半で実現したスレッド競合検出法から割込み競合検出法への拡張方式を検討し，GCC に実装した上で，小規模なプログラムを対象とする割込み競合検出実験を行った．割込み処理として C プログラムで広く利用される UNIX シグナルの処理を対象とした．小規模実験の結果，単純な拡張では，割込み処理に特有のイベント(割込みハンドラの登録/解除，多重割込み)や共有資源アクセスの観測順序によって(スレッド競合検出の文脈では生じない)誤検出または検出漏れが発生することが判明した．この問題への解決手法として割込み競合検出法に固有の高精度化手法を考案し，その成果の一部を DSW2012 で発表した．

上記 4 種のスレッド競合検出法から割込み競合の検出法への拡張は以下の通り行った．まず，スレッド処理に伴う操作（スレッドの生成/破棄，ロックによる同期）と割込み処理に伴う操作（割込みハンドラの起動/終了，マスクによる同期）の類似性に着目し，両操作間の対応関係及び割込み競合条件の定義を明らかにした．次に,各種のスレッド競合検出法において，スレッド処理に伴う操作の解析部及びスレッド競合条件の判定部を特定した後，特定した解析部と判定部を前述の対応関係に基づき割込み処理に伴う操作の解析部と割込み競合条件の判定部に改変した．これにより各種の割込み競合検出法を得た．また，多重割込みやイベント観測順序への対応策も検討しプロトタイプを試作した．

（2）スレッド競合検出法の拡張に基づく各種の割込み競合検出法の特性分析

スレッド競合検出の文脈において多様な特性（精度・効率）を示す各種の検出手法が割込み競合検出の文脈においてどのような特性を示すのかを明らかにし，高精度かつ高効率な割込み競合の検出に有望な解析手法を特定するために，以下の通り，割込み競合検出の特性分析を行った．

平成 25 年度前半は，平成 24 年度に実現した各種の割込み競合解析器の精度・効率の分析に用いる多種多様なベンチマークを作成した．このベンチマークの作成では，C プログラムのシグナル処理を対象とし，実用プログラムの開発において使用される割込み処理の典型例や開発プロジェクトのバグ履歴や CERT 等による脆弱性報告データベースを調査し，現実の開発において問題となりうる重要な割込み競合の種類を反映させることで妥当なベンチマークとなるよう配慮した．

平成 25 年度の後半は，各種の割込み競合

検出器を上述のベンチマークに適用し，割込み競合検出の精度・効率を計測した．検出精度として誤検出率（false positive rate）と検出漏れ率（false negative rate）を計測し，検出効率として割込み競合解析に伴う実行時間増加率（runtime overhead）とメモリ使用量増加率（memory overhead）を計測した．その結果，割込み競合検出の文脈に固有の特性として，検出精度と検出効率に関する以下の特性が明らかになった:

①lockset 解析（Choi ら[PLDI ’02]）の拡張に基づく割込み競合検出は，割込みハンドラの登録/破棄やアクセスイベント毎のマスク保護状況を考慮し注意深い拡張を行うと誤検出が少なく検出漏れが多い．この特性はスレッド競合検出の文脈とは異なる．

②happens-before 解析（Djit+[CCPE ’07], FastTrack[PLDI ’09]）の拡張に基づく割込み競合検出はスレッド競合検出の場合と同様に誤検出が少ない．しかし，検出漏れが極めて多い．特に,均質なサンプリング方式（Pacer[PLDI ’10]）を併用した場合にこの検出漏れの大きさが顕著となった．

③スレッド競合の文脈では，lockset 解析の誤検出を happens-before 解析の併用にて低減するハイブリッド解析（O ’Callahan ら[PPoPP ’03], MultiRace[CCPE ’07]）が有効であったが，割込み競合検出の文脈では lockset 解析拡張に happens-before 解析拡張を導入しても大きな精度改善は得られなかった．上記①で述べた通り，割込み競合検出では，注意深い lockset 解析拡張が低い誤検出率を示す．このため，happens-before 解析拡張の併用による誤検出低減効果は少なく，逆に，不健全な併用により検出漏れが顕在化する結果となった．

また，スレッド競合検出においては，検出効率化の手段としてサンプリングの併用や静的解析の併用が有効であったが，以下の通り，割込み競合検出の文脈においてはこれらの手法の併用による検出効率の向上が困難であることが分かった:

④スレッド処理に比べ割込み処理は実行の期間が非常に短い傾向がある．このため，スレッド競合検出で有効であった精度保証付き均質サンプリング（Pacer[PLDI ’10]）の素直な拡張では，検出精度を維持するために（つまり，割込み処理の短い期間内のメモリアクセスを検査対象とするために）高い率でのサンプリングを実施する必要があり大きな効率の改善は困難であった．

⑤スレッド処理に比べ割込み処理はより非同期性が高い（割込みハンドラ登録後はマスクによる保護のない任意の時点で割込み処理が発生しうる）．このため，対象プログラムの静的解析ではコードの全域に渡って割込みによる制御フローの遷移を考慮しなければならない．したがって，スレッド競合の文脈で有効であったデータフロー解析に基づく冗長検査除去による最適化法（Choi ら[PLDI ’02]）を割込み競合検出において特に大規模な検査対象プログラムに対して有効に機能させることが困難であると分かった．

（3）割込み競合検出の高精度化と高効率化に有効な解析手法の実現

各種の割込み競合検出法の特性分析結果を検討し，精度低下の要因としてスレッド競合検出の単純な拡張では多重割込みに起因する競合に対応できないことが分かった．また，多重割込みに起因する競合を漏れを抑えつつ正確に検出するには，情報量の多いメタデータ記録及び多重性の解析に特化したアルゴリズムが必要であると分かった．そこで，平成 26 年度は，割込み競合検出に特有の精度・効率向上手法として，以下の機能を実現し評価した．これらの機能の実装は平成 25 年度までに実現した lockset 解析の巧妙な拡張に基づく割込み競合解析器上に構築した．

①多重割込みの予測解析: 割込み競合検出に特有の高精度化手法として，多重割込みの予測解析手法を実現した．ある割込み A の処理中に同一の割込み A が発生し特定の関数に再入する可能性や，複数の割込み処理間での相互の割込み可能性を解析することにより，対象プログラムの実行中に観測したメモリアクセス列からより多くの潜在的割込み競合を検出する方式を実現した．

②多重割込み予測解析用メタデータ管理: 多重割込み可能性を漏れを抑えつつ正確に予測解析しようとすると，従来の lockset 解析用データ構造では多量のメタデータ記録が必要となりメモリ効率が悪い．そこで，各観測メモリアクセスイベント粒度で多重割込み可能性を高精度に判定する簡素なデータ構造を実現した．このデータ構造は割込みマスクでラベル付けされたトライ木の構造を踏襲するが各ノードのイベント表現が異なっており多重割込み競合の高精度な解析を可能にする．

③多重割込み予測解析の並列実行方式: 多重割込みによる競合の可能性を上記②のデータ構造上で逐次実行しようとすると多量の判定が必要となり実行効率が悪い．そこで，多重割込み予測解析用データ構造の各イベントノード表現を活用し複数の割込み競合の可能性を同時判定するアルゴリズムを実現した．

上記①，②，③を lockset 解析拡張に基づく割込み競合検出器に実装し，前年度までに開発したベンチマークに適用した結果，従来のスレッド競合検出の拡張による割込み競合検出器を上回る精度を得られた．特に，潜在的多重割込みの検出において大きな精度向上が得られた．また，lockset 解析の単純な拡張に基づく割込み競合検出器と比較して，実行時間はやや増加するもののメモリ使用量はほぼ同等に抑えられるという良好な結果を得た．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　0 件）

〔学会発表〕（計　4 件）
（1）荒堀喜貴，割込み競合の探査を可能にするトランザクショナルメモリ仮想化方式の検討，日本ソフトウェア科学会第 11 回 ディペンダブルシステムワークショップ (DSW2013) https://sites.google.com/site/jssstdsw/dsw2013，ポスターセッション 4-9，2013/12/27，ボテルリゾーピア熱海（静岡県・熱海市）．
（2）荒堀喜貴，並列データ処理基盤を用いた並行バグ並列検査方式の検討，情報処理学会夏のプログラミングシンポジウム 2013「ビューティフルデータ」報告集，pp.47-49，2013/08/25，アルコタワー（東京都・目黒区下目黒）．
（3）荒堀喜貴，横田治夫，トランザクショナル記号実行，情報処理学会 第 75 回全国大会大会講演論文集 2013(1)，pp.545-547，2013/3/7，東北大学（宮城県・仙台市）．
（4）荒堀喜貴，権藤克彦，ロックセット解析に基づく動的割込み競合検出の精度改善，日本ソフトウェア科学会第 10 回 ディペンダブルシステムワークショップ (DSW2012)，https://sites.google.com/site/jssstdsw/dsw2012 ，セッション 1-4，2012/12/11，理化学研究所（兵庫県・神戸市）．

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
荒堀 喜貴（Arahori Yoshitaka）
東京工業大学・大学院情報理工学研究科・助教
研究者番号：50613460

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：