1A-3

メモリバストレースによるメモリ復元手法の評価

五十嵐　史生　　望月　泰行　　黒澤　寿好
三菱電機(株)情報技術総合研究所

1. はじめに

携帯電話などの高機能な組込み機器のソフトウェア開発では、ソフトウェアが大規模化、かつ複雑化している。これにともなって、ソフトウェアの障害（バグ）も複雑化し、バグの解析負荷の増大が製品開発コストを増加させる傾向にある。

組込みシステムの開発におけるバグの解析には、ICE(In-Circuit Emulator)が利用される。ICE には一般的なデバッガの機能に加え、CPU のメモリアクセスをトレースする機能がある。メモリアクセスのトレースから任意時点のメモリイメージを復元することができれば、メモリ破壊／波及型バグ等の解析が大幅に効率化される。

本稿では、メモリを復元するアルゴリズム[3]を実装したメモリ復元ツールの評価として動作の確認を行った。なお、評価を行なうにあたり、評価用の実プログラムを ARM の評価ボード上で動作させてメモリアクセスのトレースデータを取得した。

2. メモリ復元ツール

メモリ復元ツールは、メモリ破壊/波及型バグの解析においてデータ破壊が発生した時点のメモリイメージを復元する際に利用するツールである。

2.1. 機能

メモリ復元ツールは、プログラム実行時のメモリアクセスのトレースデータをもとに、デバッグ対象プログラムの動作における任意時点でのメモリイメージを復元する。

メモリアクセスのトレースデータは、以下のデータ値からなる。

- 読出し・書込みの別
- メモリアクセス番地
- 読出み・書込みデータ

Evaluation of memory restoration from memory bus trace
Fumio IGARASHI, Yasuyuki MOCHIZUKI, Hisayoshi, KUROSAWA
Information Technology R&D Center, Mitsubishi Electric Corporation

2.2. 入出力仕様

(1) 入力
・デバッグ対象プログラム実行直後のメモリイメージ
・メモリアクセスのトレースデータ
・メモリ復元を行う時点
(2) 出力
・指定した時点のメモリイメージ

3. 評価

メモリ復元ツールが正しく動作することを確認するための評価方法、評価用のデバッグ対象プログラム、および評価結果について述べる。

3.1. 評価用のデバッグ対象プログラム

2 つの一次元配列 a、b を使った、以下に示す 2 通りのデータ操作を行うプログラムを、評価用のデバッグ対象プログラムとする。

a) コピー操作
(1) a[0]読出し
(2) b[0]書込み
(3) 同様の読出しおよび書出し操作を、全ての配列要素に対して繰り返す。

b) 入れ替え操作
(1) a[0]読出し
(2) 変数 c 書込み
(3) b[0]読出し
(4) a[0]書込み
(5) 変数 c 読出し
(6) b[0]書込み
(7) 同様の読出しおよび書出し操作を、全ての配列要素に対して繰り返す。

3.2. 評価方法

データ操作を行う評価用のデバッグ対象プログラムを動作させてメモリアクセスのトレースデータを取得する。

このデータを入力として、メモリ復元ツールを実行し、評価用のデバッグ対象プログラムの各動作ステップにおけるメモリイメージを復元する。(図 1)

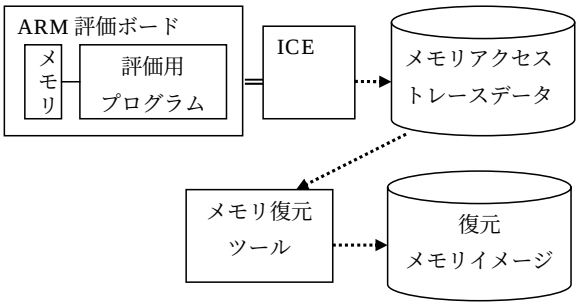

図 1 評価の流れ

3.3. 評価結果

評価用のデバッグ対象プログラムの配列要素数を 5 とした場合のメモリ復元結果を、表 1、表 2に示す。

表の各行が、3.1節の下線部分で示した各動作ステップにおけるメモリ復元の成否である。

a) コピー操作(表 1)

トレースデータ取得開始までに配列 a は初期化したが、配列 b は初期化しなかった。

配列 a については、全ての時点でメモリ復元を確認できた。配列 b については不定となる箇所があるが、これは配列 b を初期化しなかったことによるものである。

b) 入れ替え操作(表 2)

トレースデータ取得開始までに配列 a と配列 b を初期化した。

全ての時点でメモリ復元が確認できた。

表 1 コピー操作の評価結果

#	復元時点	配列aの復元結果					配列bの復元結果				
		要素0	要素1	要素2	要素3	要素4	要素0	要素1	要素2	要素3	要素4
1	a[0]読出し直後	○	○	○	○	○	不定	不定	不定	不定	不定
2	b[0]書込み直後	○	○	○	○	○	○	不定	不定	不定	不定
3	a[1]読出し直後	○	○	○	○	○	○	不定	不定	不定	不定
4	b[1]書込み直後	○	○	○	○	○	○	○	不定	不定	不定
5	a[2]読出し直後	○	○	○	○	○	○	○	不定	不定	不定
6	b[2]書込み直後	○	○	○	○	○	○	○	○	不定	不定
7	a[3]読出し直後	○	○	○	○	○	○	○	○	不定	不定
8	b[3]書込み直後	○	○	○	○	○	○	○	○	○	不定
9	a[4]読出し直後	○	○	○	○	○	○	○	○	○	不定
10	b[4]書込み直後	○	○	○	○	○	○	○	○	○	○

表 2 入れ替え操作の評価結果

#	復元時点	配列aの復元結果					配列bの復元結果				
		要素0	要素1	要素2	要素3	要素4	要素0	要素1	要素2	要素3	要素4
1	a[0]読出し直後	○	○	○	○	○	○	○	○	○	○
2	変数c書込み直後	○	○	○	○	○	○	○	○	○	○
3	b[0]読出し直後	○	○	○	○	○	○	○	○	○	○
4	a[0]書込み直後	○	○	○	○	○	○	○	○	○	○
5	変数c読出し直後	○	○	○	○	○	○	○	○	○	○
6	b[0]書込み直後	○	○	○	○	○	○	○	○	○	○
	⋮										
25	a[4]読出し直後	○	○	○	○	○	○	○	○	○	○
26	変数c書込み直後	○	○	○	○	○	○	○	○	○	○
27	b[4]読出し直後	○	○	○	○	○	○	○	○	○	○
28	a[4]書込み直後	○	○	○	○	○	○	○	○	○	○
29	変数c読出し直後	○	○	○	○	○	○	○	○	○	○
30	b[4]書込み直後	○	○	○	○	○	○	○	○	○	○

4. おわりに

メモリバストレースによるメモリ復元手法の評価として、メモリ復元ツールを実装し、一次元配列のメモリ操作を行う評価用のデバッグ対象プログラムのメモリ復元において、本ツールが正しく動作することを確認した。

今後は製品に組込まれる実アプリケーションを動作させた際の評価を実施する。

実アプリケーションを対象とした評価ではソフトウェアのサイズが大きいため、全ての時点のメモリ復元を確認することは現実的ではない。また、評価環境によっては、例えばトレースデータ取得用のバッファが小さいなど、取得できるトレースデータが制約を受けるケースも考えられる。

そこで、実際のデバッグ作業での利用に的を絞り、以下の評価を行う予定である。

- メモリ復元の結果、不定となる箇所の割合
- メモリ復元に必要なトレースデータの量
- 速度性能

参考文献

[1]アーム(株), ARM アーキテクチャリファレンスマニュアル, http://www.jp.arm.com/

[2]アーム(株), ETM9 テクニカルリファレンスマニュアル, http://www.jp.arm.com/

[3]望月他,メモリバストレースによるメモリ復元手法の検討,情報処理学会第 69 回全国大会