A-12

QEMU を利用した V850 シミュレータの評価

Evaluation of V850 simulator using QEMU

中本 幸一†　　薮内 健二‡　　尾崎 辰典§
Yukikazu Nakamoto　Kenji yabuuchi　Tatsunori Ozaki

１．はじめに

自動車や航空機はいまや小型のコンピュータがネットワークで結合された大規模分散組込みシステムとなってきている．こうしたコンピュータシステム，特にソフトウェアの規模や複雑さが最近急速に増大している．さらに，これらのシステムは高信頼性，高環境性が要求され，そのため開発コストも膨大である．分散組込みシステムは多種類の CPU や物理空間と制御を行うデバイスから構成されること，さらに大規模なネットワークシステムであることが特徴である．このような高性能な大規模分散システムを高い生産性と品質を保持して開発するためには分散組込みシステムの仮想実行環境が必要となる[3]．この仮想実行環境では多数の CPU シミュレータをネットワークで結び，様々なデバイスシミュレータを統合することで，分散組込みシステムの仮想実行環境を提供する．

筆者らはこの仮想実行環境における CPU シミュレータを，ターゲット CPU を NEC 製プロセッサ V850 として，QEMU と呼ばれる CPU シミュレータを用いて開発した[7]．本稿では，その評価を報告する．

２．QEMU

本研究で使用した QEMU は Fabrice Bellard によって開発されたオープンソースの CPU シミュレータである[1]．より正確には QEMU は命令変換型の CPU シミュレータを生成するジェネレータで，生成された CPU シミュレータは Linux，Windows，MacOS，FreeBSD のようなオペレーティングシステム上でアプリケーションとして動作する(図 1 参照)．

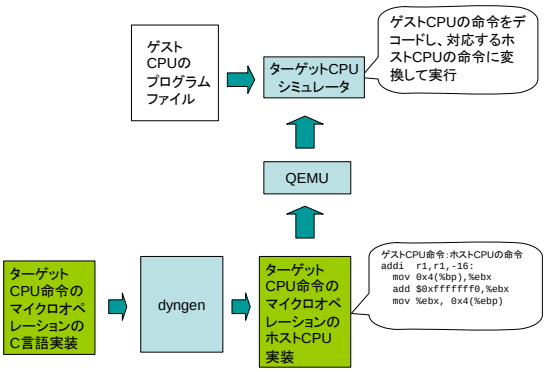

図 1　QEMU の処理フロー

† 兵庫県立大学大学院応用情報科学研究科
‡ (株)オクトパス
§ 兵庫県立大学大学院応用情報科学研究科
(現在，富士通テン(株))

命令変換型なのでターゲット命令の高速な実行が期待できること，命令多くのターゲット CPU をサポートしているので多種の CPU を利用する分散組込みシステムの構築が容易になること，さらに，新たなマシン記述とエミュレートデバイスを加えることで特別な組込み機器を簡単にシミュレートすることができること，などの特徴を有する．

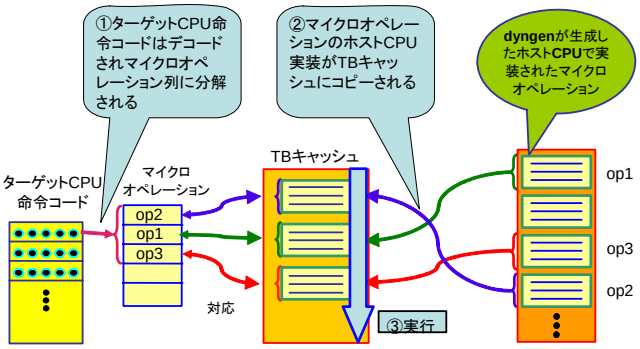

図 2　QEMU の命令変換

QEMU における命令変換は，実行時にターゲット CPU の命令をホスト CPU 用に変換することによってシミュレーションを行う(図 2 参照)．この変換方法は，まず，ターゲット CPU の命令をマイクロオペレーションの列に分割する．QEMU でのマイクロオペレーションは，ターゲット CPU より単純な命令であり，ホスト CPU の命令列にコンパイルされて QEMU のシミュレータ内に組み込まれる．QEMU 実行時に，まずターゲット命令の命令変換結果が Translated Block(TB)キャッシュというキャッシュ内に存在するか調べる．存在しない場合は，ターゲット命令コードがデコードされ，対応するマイクロオペレーションの列に分解する(図 2①)．分解されたマイクロオペレーションに対応するホスト CPU の命令列が TB キャッシュにコピーされる(図 2②)．この命令変換はターゲットプログラムにおいてジャンプ等の命令が現れるまで続けられる．ターゲット命令コードのデコードとマイクロオペレーションのコピーが終了すると，当該 TB キャッシュの先頭からプログラムが実行される(図 2③)．ターゲット命令の命令変換結果が TB キャッシュ内にある場合はその変換結果がそのまま再利用され，実行される．

3．V850/V850E1 の概要

V850 は NEC 製の組込み用 CPU で，シングルチップ・マイクロコンピュータである[4]．V850 はユーザーモード(プロテクション)のない RISC プロセッサである．また命令数は 74，32 ビット汎用レジスタは 32 本，ロング/ショート形式を持ったロード/ストア命令，3 オペランド命令，プログ

ラム空間は 16M バイト・リニア，データ空間は 4G バイト・リニア，飽和演算命令，ビット操作命令といった特徴を持つ．V850E1 は，V850 に C 言語の switch 文処理，スタック・フレームの生成／削除などの命令が追加されたものである[5].

4. V850 QEMU の評価

上述の V850 ，V850E1 プロセッサを QEMNU を利用してシミュレータを開発した[7]．この V850 QEMU をベンチマークプログラムを使用して，命令実行速度とメモリアクセス速度を評価した．

4.1 命令実行速度

Dhrystone[6]の 2.1 を使用して命令実行速度を測定した．測定結果を表 1 に示す．測定環境は，Pentium DualCore / 2.2G (E2200)，メモリ 2GB，OS は Ubuntu 9.04，x86 ネイティブのコンパイラは gcc 4.3.3，V850 のクロスコンパイラは v850-elf-gcc (GCC) 3.4.6 である．

表 1: Dhrystone による実行結果

評価対象(TBサイズ)	平均	標準偏差
QEMU V850(16MB)	58450	546
QEMU V850E1(16MB)	81094	3441
QEMU V850E1(なし)	1946	138
ネイティブ x86	6752154	510201

今回の評価環境での TB キャッシュ全体のサイズは 16MB で，TB の個数は 128K 個である．Dhrystone のプログラムは 1 回のデコードで全て TB にバッファリングされている．このため，ターゲット命令コードの変換結果が TB キャッシュにある場合は，それがない場合に比べて命令実行速度が約 40 倍高速であるということができる．TB キャッシュの効果は大きいと考えられる．また，V850E1 QEMU の Dhrystone MIPS 値は，約 45 MIPS と見積もることができる．

4.2 メモリアクセス

メモリアクセス速度を評価するために性能測定ベンチマークである LMbench[2]を使用した．LMbench においてメモリのアクセスを評価するプログラム bw_mem から rd, wr, rdwr, mcp の部分を抜き出して実行した．rd，wr，rdwr，mcp はそれぞれ，同一アドレスからの読み，書き，読み書き，あるアドレスから読み異なるアドレスへの書き込みに対応する．オリジナルの LMbench では 16 バイトおきにアクセスしたものであったので，本評価ではさらに全てのアドレスにアクセスする評価も行ってみた．読み書きするデータのサイズは 8MB である．評価環境は Dhrystone と同じである．その結果を表 2 に示す．表の各測定結果の上段は 16 バイトおき，下段は全てのアドレスをアクセスした場合の値，各数値の単位は GB/s である．

表 2: LMbench による実行結果

評価対象	rd	wr	rdwr	mcp
QEMU V850E1	0.321	0.495	0.227	0.043
	0.100	0.180	0.028	0.012
ネイティブ x86	2.40	1.17	1.02	0.81
	1.97	1.12	0.74	0.76

この結果から分かるのは，QEMU とネイティブ間のメモリアクセス比率が 20 から 60 倍程度であり，4.1 節の命令実行速度の比率 80 倍と比べて小さいことである．これはネイティブでのメモリアクセス時の待ちが QEMU では他のメモリ処理で見えなくなっているなどの理由が考えられる．

5. おわりに

本稿では，QEMU による V850 シミュレータの評価について述べた．

今回の試作評価から分かったことは，QEMU による命令変換型シミュレーションは高速である．一方，命令変換結果が再利用できない場合は 40 倍ほど遅くなり，ジッタが大きい点がターゲットプログラムのリアルタイム処理を行う場合に課題である．これを解決する手段として，ターゲットプログラムの周期実行を QEMU で同期実行させ，その周期の間にジッタの吸収や入出力処理を行うことを考えている．

謝辞

本研究は科学研究補助金基盤研究(C)(21500040)と富士通テン(株)の支援を受けています．

参考文献

[1]Bellard, F.: QEMU, a Fast and Portable Dynamic Translator, *Proc. USENIX 2005 Annual Technical Conference*, pp. 41-46 (2005).

[2]McVoy, L. and Staelin, C.: LMbench - Tools for Performance Analysis. http://www.bitmover.com/lmbench/.

[3]Nakamoto, Y., Abe, I., Osaki, T., Terada, H. and Moriyama, Y.: Toward Integrated Virtual Execution Platform for Large-scale Distributed Embedded Systems, *Proc. 6th IFIP WG 10.2 International Workshop, Software Technologies for Embedded and Ubiquitous Systems*, pp. 317-322 (2008).

[4]NEC: V850 ファミリ 32 ビット・シングルチップ・マイクロコンピュータ ユーザマニュアル アーキテクチャ編 (1994).

[5]NEC: V850E1 32 ビット・マイクロプロセッサ・コア ユーザマニュアルアーキテクチャ編 (1999).

[6]Weicker, R.: Dhrystone: A Synthetic Systems Programming Benchmark, *Communications of the ACM*, Vol. 27, No. 10, pp. 1013-1030 (1984).

[7] 中本幸一，尾崎辰典，藪内健二 ：QEMU を利用した V850 シミュレータの開発と評価，情報処理学会研究報告，Vol.2009-EMB-014, No.9 (2009).