

## Modificações no MIPS Inspiradas na Intel VT-x para Suporte à Virtualização Utilizando ArchC\*

Manuela K. Ferreira, Henrique C. Freitas, Philippe O. A. Navaux

Instituto de Informática Universidade Federal do Rio Grande do Sul (UFRGS)  
Caixa Postal 15.064 91.501-970 Porto Alegre RS Brazil  
{mkferreira, hcfreitas, navaux}@inf.ufrgs.br

**Resumo.** *Este artigo descreve as modificações realizadas no modelo MIPS em ArchC versão 1.6 para oferecer suporte de hardware à virtualização. As instruções e estruturas acrescentadas foram inspiradas no conjunto de instruções da tecnologia Intel VT-x. O objetivo deste artigo é apresentar uma arquitetura de processador MIPS com suporte à virtualização para simulação de aplicações utilizando o ArchC.*

### 1. Introdução

A virtualização pode ser vista como a capacidade de executar múltiplos Sistemas Operacionais (SOs) em uma única plataforma física, dividindo os recursos de hardware. Em outras palavras, a virtualização permite ter dois ou mais computadores virtuais, executando SOs e aplicações diferentes ao mesmo tempo em um mesmo computador.

O uso da virtualização tem se tornado comum para aumentar o aproveitamento dos recursos físicos dos sistemas. Assim, cada vez mais esforços são direcionados para o aumento do desempenho de sistemas virtualizados. Para alcançar esse objetivo, existem diversas abordagens em software e, mais recentemente, em hardware.

Este artigo descreve o conjunto de modificações feitas em um processador MIPS modelado em ArchC para oferecer suporte de hardware à virtualização, apresentando quais instruções e estruturas foram acrescentadas ao modelo. As modificações aqui propostas são fortemente inspiradas no conjunto de instruções dos processadores da Intel com tecnologia Intel VT-x. O objetivo é oferecer uma arquitetura de processador MIPS com suporte à virtualização para simulação de aplicações em projetos de pesquisa.

Primeiramente é apresentada a ferramenta de simulação ArchC. Após, é descrito o conjunto de instruções da tecnologia Intel VT-x. Então, é apresentado o modelo original do MIPS, feito em ArchC versão 1.6, seguido pela descrição das modificações feitas para oferecer suporte de hardware à virtualização.

### 2. ArchC

O ArchC é uma linguagem de descrição de arquiteturas para a geração automática de simuladores utilizando para isso outra ferramenta, o SystemC.

O SystemC é um conjunto de classes em C++ que estendem a linguagem para permitir a modelagem de hardware e sistemas.

---

\* Apoiado pela empresa Microsoft.

O objetivo do ArchC é facilitar a utilização do SystemC, fornecendo uma interface mais abstrata que utiliza informações estruturais e do conjunto de instruções da arquitetura para geração automática de simuladores [Rigo, Azevedo, Araújo e Centoducate 2005].

### 3. Intel VT-x

A tecnologia Intel VT-x consiste em um conjunto de instruções e registradores, denominado *Virtual Machine Extensions* (VMX), para suporte à virtualização em arquiteturas IA-32. Além da Intel, a AMD também possui suporte de hardware em seus processadores, entretanto, as extensões feitas pela tecnologia AMD Pacifica são muito semelhantes às vistas aqui, seguindo os mesmos princípios.

VMX inclui a oferta de dois novos modos de operação da CPU chamados VMX *root*, onde o Monitor de Máquina Virtual (MMV) executa, e VMX *non-root*, onde os SOs convidados executam. Ambos suportam todos os quatro níveis de privilégio [Uhlig e Neiger 2005], como pode-se ver na Figura 1, permitindo que os SOs convidados executem em um nível zero de privilégio e acreditem que possuem o controle da CPU.

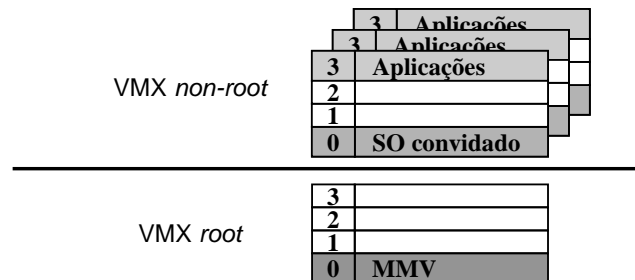


Figura 1. Modo VMX *root* e VMX *non-root* [Uhlig e Neiger 2005].

Esta tecnologia define duas novas transições: **MV entrada** (*VM entry*), que é a transição do modo VMX *root* para o modo VMX *non-root*, e **MV saída** (*VM exit*) que faz a transição inversa [Uhlig e Neiger 2005], veja Figura 2. Também é disponibilizada uma nova estrutura de dados, o *Virtual Machine Control Structure* (VMCS). Cada Máquina Virtual (MV) gerada possui o seu VMCS para guardar o seu contexto, sendo que apenas um deles será o **VMCS ativo**. Com a configuração do VMCS é possível definir quais instruções irão causar **MV saídas** [Uhlig e Neiger 2005].

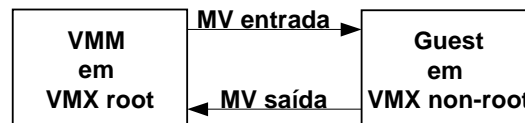


Figura 2. MV entrada e MV saída.

Cada **MV entrada** irá salvar o estado da CPU na área de estado do hospedeiro no VMCS e carregar o novo estado da área de estados do convidado no VMCS. A **MV saída** irá salvar o estado do processador na área de estado do convidado no VMCS e carregar o estado da área de estado do hospedeiro no VMCS [Uhlig e Neiger 2005].

As novas instruções fornecidas pela VMX são [Intel Corporation 2005]:

- **VMXON** e **VMXOFF**: para, respectivamente, ativar e desativar as extensões VMX;
- **VMLAUNCH**, **VMCALL** e **VMRESUME**: para criar um VMCS e lançar uma nova máquina virtual, entrando no modo VMX *non-root*, para sair do modo VMX *non-root* e para retornar ao modo VMX *non-root*, respectivamente;
- **VMCLEAR**, **VMPTRLD** e **VMPTRST**: para, respectivamente, limpar o VMCS ativo, salvar a referência para o VMCS ativo na memória e carregar uma nova referência de VMCS da memória;
- **VMREAD** e **VMWRITE**: para, respectivamente, ler e escrever dados no VMCS ativo;

#### 4. Modelo Original do MIPS com ArchC

O modelo original, em ArchC versão 1.6, criado para simulação do processador MIPS R3000 está disponível em [ArchC Org 2007]. Essa é a versão com os 5 estágios de *pipeline* do MIPS. O modelo implementa os 32 registradores de 32 bits para uso geral. Também possui os registradores hi e lo, que juntos somam 64 bits, para operações de divisão e multiplicação.

Nesse modelo do MIPS, não foram implementados os registradores de coprocessamento, como o registrador de nível de privilégio de CPU. Como esses registradores não estão presentes, as instruções para acesso a esses registradores também não estão presentes, como é o caso da instrução de MOV.

O modelo possui todas as instruções aritméticas e de desvio do MIPS implementadas. A instrução SYSCALL e BREAK estão modeladas, mas não estão implementadas, provocando a parada da simulação se executadas.

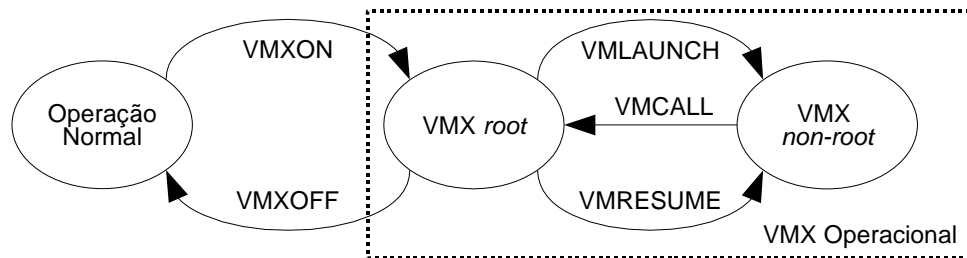
#### 5. MIPS com Instruções de Virtualização

O MIPS com instruções de virtualização, denominado aqui como MIPS-vt, surge de um conjunto de acréscimos que foram feitos no modelo original do MIPS, visto na seção anterior. As novas estruturas e instruções acrescentadas são inspiradas na tecnologia Intel VT-x.

Foi adicionada uma estrutura de VMCS, que possui sua referência localizada na memória, mas é uma estrutura específica do processador para armazenamento do contexto de cada MV.

Também foi adicionado um novo banco de quatro registradores para controle dos modos de virtualização. Esses registradores possuem 32 bits para permitir o aproveitamento das instruções originais do MIPS projetadas para registradores de 32 bits. Dois desses registradores guardam as referências para o VMCS ativo e para o VMCS do MMV. Os outros dois, registram se o processador está em modo VMX *root* ou VMX *non-root* e se as extensões VMX estão ativadas.

Em relação às instruções, foi acrescentado um subconjunto das instruções VMX. As instruções acrescentadas são dos tipos já definidos no MIPS original, elas são: VMXON, VMXOFF, VMLAUNCH, VMRESUME, VMCALL, do tipo Type\_R; VMCLEAR, VMPTRLD e VMPTRST, do tipo Type\_I.



**Figura 3. Transições provocadas pelas instruções de virtualização do MIPS-vt.**

Como pode ser visto na Figura 3, a instrução VMXON passa do modo normal de operação do processador, para o modo VMX *root*, onde as outras instruções VMX são reconhecidas. A instrução VMXOFF apenas volta para o estado normal. A cada invocação da instrução VMLAUNCH é criado um novo VMCS referenciado pelo registrador que indica o VMCS ativo e o processador entra no modo VMX *non-root*. A instrução VMCALL provoca a saída do modo VMX *non-root*, que pode ser provocada também pela execução de alguma instrução que não seja permitida nesse modo. Com a invocação da instrução VMRESUME ocorre a retomada da execução da MV a partir do estado salvo no VMCS ativo. O formato dessas instruções é formado pelo nome da instrução em minúsculo, sem parâmetros.

A instrução VMPTRLD carrega uma referência de VMCS da posição de memória passada como parâmetro para o registrador de VMCS ativo. A instrução VMPTRST salva a referência do VMCS ativo na posição de memória passada. E o VMCLEAN limpa o VMCS cuja referência na memória foi passada como parâmetro. Essas instruções têm o formato "<nome da instrução em minúsculo> %imm(%reg)".

## 6. Conclusões

Este artigo apresentou as extensões feitas no MIPS R3000 em ArchC 1.6 para oferecer suporte à virtualização com o objetivo que esse modelo seja utilizado para simulações em pesquisas.

Como trabalhos futuros pretende-se estender o MIPS-vt para incluir instruções para a virtualização em um contexto *multi-core*.

## Referências

- ArchC Org (2007) "The ArchC Architecture Description Language", <http://www.archc.org>, dezembro.
- Intel Corporation (2005) "Intel Virtualization Technology Specification for the IA-32 Intel Architecture", <http://www.intel.com/cd/ids/developer/asmo-na/eng/197666.htm>, dezembro.
- Rigo, S., Azevedo, R., Araújo G., Centoducate, P. (2005) "ArchC - Construção de Modelos de Processadores Usando uma Linguagem de Descrição de Arquiteturas", Laboratório de Sistemas de Computação (LSC) IC-UNICAMP.
- Uhlig, R. e Neiger, G. (2005) "Intel Virtualization Technology", Computer Journal, v. 38, p.48-56.