

一种软硬件结合的新型嵌入式模拟器

周明君,许武军,梁 威,禹素萍,范 红

(东华大学 信息科学与技术学院,上海 201620)

摘 要: 介绍一种以软硬件结合取代纯软件模拟外设的新型的嵌入式模拟器的设计与实现. 通过以软硬件结合替代软件,达到更准确的外设模拟. 并吸取软件模拟的优势,提供了模拟 CPU 可以改变而硬件接口不需改变的模拟方式. 模拟器内核以解释执行、地址空间抽象等方法为模拟器提供了良好的模拟准确性和可配置性. 通过实验验证了这种方式比单纯的软件实现具有更好的效率.

关键词: ARM 模拟器; 二进制解释执行; 硬件接口; 地址空间

中图分类号: TP311

文献标识码: A

文章编号: 1000-7180(2014)11-0125-04

A Novel Embedded Emulator Consisting of Software and Hardware

ZHOU Ming-jun, XU Wu-jun, LIANG Wei, YU Su-ping, FAN Hong

(College of Information and Technology, Donghua University, Shanghai 201620, China)

Abstract: Introduce a kind of design and implementation for an emulator using hardware instead of software to handle peripheral emulation. Benefiting from the hardware, the emulator improves the accuracy. Besides, it can change the core CPU type without changing the hardware interface. The core of the emulator provides accurate and scalable emulation by using binary interpretation and abstract of address space. The efficiency was proved to be better than that of the pure software implementation through experiment.

Key words: ARM emulator; binary interpretation; hardware interface; address space

1 引言

模拟器技术是一种主要由计算机软件模拟其他平台软件或硬件的技术. 通常可以分为全系统模拟与功能性模拟. 无论哪种模拟方式,在已实现的模拟器中,常常通过纯软件进行模拟. 例如当需要模拟一种外部设备时,就使用软件生成一个虚拟的外部设备,在电脑界面上给予直观的显示,常见的模拟器 QEMU^[1]、Skyeye^[2] 和 SimOS^[3] 都采用了这种方式. 这种方式能够提供功能性的模拟,但对于实际电路的电信号分析无能为力. 本文提出一种由软硬件结合的模拟器技术,使得由计算机软件模拟的处理能够接入到实际的外部设备中,从而实现对外部设备的精确调试.

2 系统结构

本系统模拟一个 ARM Cortex-M^[4] 系列内核的 CPU,程序运行平台为 X86 架构的 PC,主要由 C 语言编写而成. 不同于常见软件模拟器的纯软件实现,本系统主要分为由软件实现的核心部分和硬件实现的外设部分,如图 1 所示. 其中核心部分完成指令集模拟、中断模拟、外设 IO 请求、地址空间管理模拟等工作,而外设部分则完成将软件 IO 请求转换为真实外设接口的工作.

外设部分实际上是一个硬件 IO 接口部件,通过 USB 与 PC 相连. 在模拟器与此部件中定义了一种简单的协议,使两者进行通信. 实际上,硬件部分与软件部分并非紧密耦合,软件可以选择使用硬件接口,也可以不使用;同样如果其他模拟器实现了同

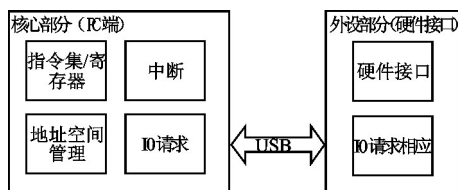


图1 模拟器系统架构

样的协议,也可以与此硬件接口进行通信。

3 核心部分的设计与实现

核心部分完成对 CPU 内核的模拟,它模拟了一个完整的 CPU 的主要部件.这些部件完全由软件实现,这意味着可以通过软件模块的装载和卸载达到更改 CPU 内核的目的。

3.1 指令集与寄存器

指令集模拟有基于解释和基于翻译^[5]两种方式.这里主要通过解释执行的方式进行模拟.解释执行是一种基本的指令集模拟方式,它对每条指令都执行取指令、翻译、执行三个步骤,顺序地解释每一条指令.这种方式实现简单,并且模拟准确性较高.出于对准确性的要求,本模拟器在指令集部分采用这种简单可靠的方式。

对上层而言 CPU 实际上就是一些寄存器的组合,它们包含了 CPU 在运行过程中的各种状态,而在 ARM 中表现为 R0-R14、PC、PSR 等寄存器.因此通过一个包含模拟寄存器的结构就能够表示一个运行中的模拟 CPU。

在实际指令集的实现中,并不直接将 ARM 指令集翻译为 X86 指令集,而是采用一张函数指针表实现,其中每一项代表一条指令的执行函数,借助于编译器将这些函数翻译为本地的 X86 指令.每条指令通过查表、执行就能够改变模拟寄存器组的值。

在 ARM 指令集中,每条指令都类似有如下结构:

[指令集标识][指令标识][操作数]

通过指令集标识识别属于 Thumb 或 ARM 指令集.指令标识则用来确定一条特定的指令.但 ARM 指令集中,指令标识并不是一个固定的位域.因此,通过一张表来确定所有的指令会浪费大量的空间.在本系统中,将指令集进行分类,对译码格式相近的指令集使用一张单独的译码表,从而将整个指令集分为若干级子表.尽管这使得在查表过程中损失了一小部分性能,但大大提高了内存的利用。

3.2 中断

中断也是模拟器必不可少的部件之一.在每个

模拟周期的结束检测中断是普遍采用的做法.这种方式与解释执行可以很好地协调,并且能够快速响应中断.本系统实现了 Cortex-M 系列独有的嵌套向量中断控制器(NVIC).它能够支持大量中断向量,并支持嵌套和优先级,比传统的 ARM 中断控制器更复杂。

中断的实现会很大程度上影响一个模拟器的执行效率,如果将大部分时间用于检测中断会大大降低模拟器的执行效率.在本系统中,中断通过一个简单的优先队列实现.在模拟器的其他部分中,每当产生中断,便将中断加入到此优先队列中.通过将中断号及其优先级组合,得到其在优先队列中的优先级,减少不必要的优先级判断。

在每个指令周期的末尾检查中断队列,当没有中断产生时,此队列为空,即可跳过剩余的检测,减少中断检测时间.而有中断产生时只需获得优先级最高的中断,并执行相应的中断服务例程。

3.3 地址空间

由于 ARM 采用统一寻址的方式对外设和内存进行编址,因此在设计中,对所有 IO 的模拟都基于同一个抽象接口,从而可实现对地址空间的动态配置。

地址空间的模拟通常可以使用一个数组来实现,但这样导致编码冗余性大增,也降低了系统的可扩展性.为兼顾扩展性和效率,这里使用一棵查找树对整个地址空间进行管理.树中的每个元素代表一个内存区域或外设寄存器空间,具有类似以下的结构:

```

struct memory_area{
    int start_addr, size;
    int (* read)(uint32_t offset, uint8_t *
buffer, int size, struct memory_area * region);
    int (* write)(uint32_t offset, uint8_t *
buffer, int size, struct memory_area * region);
};
  
```

通过 read 和 write 两个函数指针接口,每个外设都可以拥有自己的读写方法.通过这个结构可以挂载不同的外设或内存.每当读取或写入某个地址,模拟器先通过查找树找到对应的 struct memory_area,再调用其 read 或 write 接口。

由于这些接口的存在,通过实现不同的接口函数,可以动态增减外设.对于同一个外设,通过同时实现软件模拟接口和硬件 IO 接口,可以使得用户自行选择外设的模拟方式。

4 外设部分的设计与实现

4.1 外设的模拟方式

在常见的软件模拟器中,外设也以软件的形式存在并被调用.在这种方式中,软件外设需要与CPU内核进行同步,有两种常用的方式^[6]:串行方式、并行方式.串行方式通过在每个模拟指令周期最后检查每个外设,并执行相应的动作;并行方式通过为每个外设建立单独的线程以减少对CPU的消耗.

由于这些方式都是基于软件的模拟,因此无论哪种方式都会随着外设的数量增加而不断消耗CPU资源,并且这些方式都不能非常准确地模拟外设,特别是在调试某些通信协议、接口的时候.由于外设接口通常是标准的,因此可以采用硬件IO接口部件与模拟CPU协同处理外设请求,不仅不影响模拟器的扩展,并且能有效地解决以上问题.

4.2 外设连接协议

外设部分通过USB连接PC与硬件IO接口部件.IO接口部件通过USB上层协议与模拟器软件进行通信,并将IO请求转换为真实的接口操作.由于不同CPU对应的IO接口不同,因此在运行初期需要对片内外设所对应的硬件IO接口部件进行映射.

对于不同的外设而言,在read和write的具体实现中,可以与具体的硬件IO接口部件通过USB进行通信.为简单起见,其间的协议为一种面向字节的协议,每个协议包具有以下结构:

[接口类型ID]+[接口编号]+[数据包类型]+[内容]

硬件IO接口部件中的固件根据协议包的内容,将不同的数据包通过不同的接口进行发送.当硬件接口产生中断时,硬件IO接口部件会将中断信息发送给软件模拟器.在软件模拟器中存在一个单独的线程对硬件IO接口部件产生的中断进行轮询,一旦发现有中断,便会将此中断加入到模拟器的中断队列中.

只要遵循这样的协议,无论软件CPU内核如何变化,硬件IO接口部件都无需发生变化,这样充分利用了软件模拟器的优势.

4.3 外设硬件实现和中间层

硬件IO接口部件由NXP LPC1788作为其主控,此SOC提供了许多常用的接口,如I2C、SPI、网口、USB等等.同时也配置了一些常见的外设如

LED等.它的固件通过不断接收USB命令、解析命令和转换为实际接口配置命令进行工作.硬件主要结构如图2所示,其主要流程如图3所示.

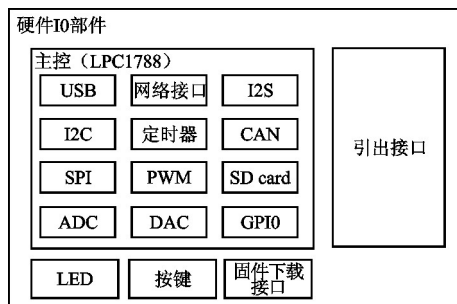


图2 硬件结构

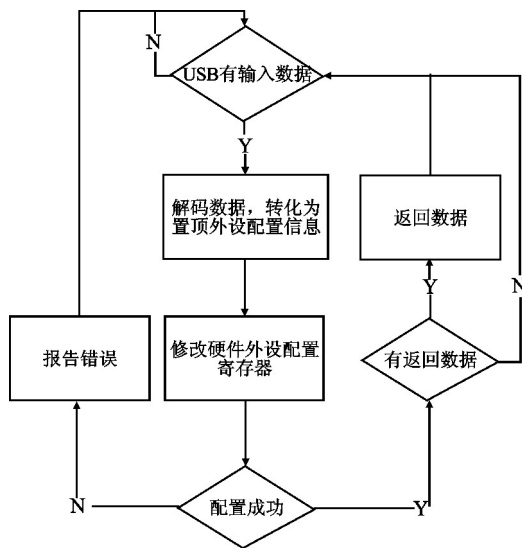


图3 硬件固件流程

为了使模拟器能更好地扩展,也由于不同CPU的同一类接口所提供的配置寄存器不尽相同.例程提供了一个中间层,实现了访问硬件IO部件的接口函数,在特定CPU的实现时可以对这些接口函数进行组合.

除此之外,中间层也提供了对同一类型外设功能的抽象,例如,对IO端口提供输入输出配置、输入输出数据控制;对LCD显示提供方向控制、同步控制、显存控制;对定时器提供开始、停止、清零、匹配等接口例程.以便于添加具有不同配置寄存器的统一类型的外设,降低扩展难度.

5 系统测试

由于本系统同时实现了软件和硬件的外设模拟方式,所以系统测试时,针对两种不同的模拟方式进行测试对比.主要测试项有中断响应准确性、软件内

存占用、模拟 CPU 速度等。

中断响应准确性由定时器中断产生的时间间隔为实际测试项,通过对每两次定时器中断产生的时间间隔与理论定时时间的偏差取平均,取得中断响应的准确性指标。

软件内存占用由两种方式稳定运行时的平均内存占用为指标。

模拟 CPU 速度由两种方式全速运行相同程序时的实际平均指令频率为指标。

由表 1 的测试结果可以发现,硬件模拟无论在中断响应准确性还是内存占用、模拟 CPU 速度方面都优于软件模拟。究其原因是软件模拟外设过程中需要更多的内存结构和判断,从而拖累了模拟器的执行效率。在中断响应时也是同理,由于其他外设线程的运行,从而降低了中断响应的实时性。而硬件模拟时,模拟器仅需要 2 个执行线程:主线程和模拟中断线程,其余交由硬件处理,从而提高了中断响应的实时性。

表 1 测试结果

测试项	软件模拟	硬件模拟
定时器中断平均时间偏差/ms	12.5	8.2
内存占用(共打开 5 个外设)/kB	926	583
模拟 CPU 速度(kIPS)	230.1	251.6

6 结束语

本模拟器采用了软件与硬件相结合的方式进行了模拟,不仅能对软件实现的外设进行直观的显示,也能够连接实际硬件设备,达到更加逼真的模拟效果。

硬件模拟虽然需要额外的硬件,但由于软件核心可以变化,实际并不增加过多成本,但其带来了与

外围硬件连接的能力及更好的模拟器效率。

由于上述原因,对于嵌入式处理器,本模拟器在理论验证和实验使用中都优于传统软件模拟器。

参考文献:

- [1] Bellard F QEMU. A fast and portable dynamic translator[C]// USENIX Annual Technical Conference. [s. l.]:FREENIX Track, 2005: 41-46.
- [2] 王利明,宋振宇,李明,等. 一个开放源码的嵌入式仿真环境—SkyEye[J]. 单片机与嵌入式系统应用, 2003(9): 14-18.
- [3] Rosenblum M, Herrod SA, Witchel E, et al. Complete computer system simulation: The SimOS approach[J]. IEEE Parallel and Distributed Technology: Systems and Applications, 1995, 3(4): 34-43.
- [4] Cop ARM. Cortex-M3 Technical Reference Manual [R]. ARM DDI0403, 2010.
- [5] 张激,李宁波. 基于二进制翻译的仿真器关键技术研究[J]. Computer Engineering, 2010, 36(16): 246-248.
- [6] 邓立波,龙翔,高小鹏. ArmSim 全系统模拟器的设计与实现[J]. 微计算机信息, 2008, 1(2): 9-14.
- [7] 王海晨,赵祥模. 应用基于抽象机的动态翻译设计 Java 处理器[J]. 微电子学与计算机, 2012, 29(7): 1-3.

作者简介:

周明君 男,(1990-),硕士研究生.研究方向为嵌入式系统.
许武军 男,(1972-),博士,副教授.研究方向为智能穿戴系统、嵌入式计算等.
梁威 男,(1989-),硕士研究生.研究方向为嵌入式系统.

(上接第 124 页)

- [7] 单冬红,赵伟艇. 基于主成分分析的神经网络入侵检测仿真研究[J]. 计算机仿真, 2011, 28(6): 153-156.
- [8] 李亚荣,刘东东,郑腾飞. 基于序列图像的运动目标快速检测技术的研究[J]. 电子技术与软件工程, 2014(3): 117-118.
- [9] Jian-liang Zhang, Zhen-yang Wang, Xiang-dong Xing, et al. Effect of aluminum oxide on the compressive strength of pellets[J]. International Journal of Miner-

als, Metallurgy and Materials, 2014, 2(4): 339-344.

- [10] 于凯. 数字图像边缘特征提取方法及研究[J]. 中国科技纵横, 2014(5): 49-49.

作者简介:

王佳欣 男,(1983-),硕士,讲师.研究方向为计算机应用.
文政颖 女,(1979-),硕士,讲师.研究方向为计算机应用与图像处理.