面向 SoC 系统芯片中跨时钟域设计的模型检验方法

冯 毅,易江芳,刘 丹,佟 冬,程 旭
(北京大学微处理器研究与开发中心,北京 100871)

摘 要: 传统方法无法在 RTL 验证阶段全面验证 SoC 系统芯片中的跨时钟域设计. 为解决此问题,本文首先提出描述亚稳态现象的等价电路实现,用以在 RTL 验证中准确体现亚稳态现象的实际影响;然后使用线性时序逻辑对跨时钟域设计进行设计规范的描述;为缓解模型检验的空间爆炸问题,进一步针对跨时钟域设计的特点提出基于输入信号的迁移关系分组策略和基于数学归纳的优化策略. 实验结果表明本文提出的方法不仅可以在 RTL 验证阶段有效地发现跨时钟域设计的功能错误,而且可以使验证时间随实验用例中寄存器数量的递增趋势从近似指数级增长减小到近似多项式级增长.

关键词: 形式化验证; 模型检验; 跨时钟域设计; 线性时序逻辑
中图分类号: TP302 **文献标识码**: A **文章编号**: 0372-2112 (2008) 05-0886-07

Model Checking on Clock Domain Crossing Design of System-on-Chip

FENG Yi, YI Jiang-fang, LIU Dan, TONG Dong, CHENG Xu
(Micro-Processor Research and Development Center, Peking University, Beijing 100871, China)

Abstract: Traditional approach in RTL verification cannot completely verify the clock domain crossing (CDC) design of SoC. To solve this problem, we first propose a RTL module to model the actual effect of metastability. Then, linear temporal logic is proposed to model the specification of CDC designs. To solve the exponential problem in model checking, based on the characteristic of CDC designs, a strategy on input signal partition for the state transition's characteristic function and a strategy on induction are proposed. Experiment results demonstrate that our method is useful to find CDC errors in the RTL verification stage and the verification time is approximately reduced from exponential to polynomial increased with the register size.

Key words: formal verification; model checking; clock domain crossing design; linear temporal logic

1 引言

随着半导体器件集成度的提高,系统芯片(System-on-Chip, SoC)中集成了越来越多的 I/O 控制器,例如 DDR 控制器、Flash 控制器、USB 控制器和 PCI 桥接器等[1]. 由于接口协议的规定以及对系统高性能和低功耗的需求,这些 I/O 控制器通常工作在不同频率的异步时钟域中.

各控制器之间的数据访问,需要在异步时钟域之间进行数据传输,处理跨时钟域(Clock Domain Crossing, CDC)数据传输的电路结构被称为跨时钟域设计. 在跨时钟域路径上传递信号可能会导致路径终点寄存器的建立或保持时间违例(Setup/ Hold Timing Violation),从而引起该寄存器的输出端进入亚稳定状态(Metastability). 尽管加入同步器(Synchronizer)可以消除寄存器输出端的亚稳态现象,但其输出体现输入变化的确切时钟周期仍然不可预测,因此由亚稳态引起的跨时钟域设计的功能错误并不能仅通过简单地加入同步器而消除.

功能验证是 SoC 系统芯片设计流程中最耗时的工作,占整个设计周期的 50 %～80 %[2],其目的是检验设计实现是否与设计规范相一致. 对于寄存器传输级(Register Transfer Level, RTL)的设计实现方法,功能验证主要分为模拟验证和形式化验证. 然而,传统验证方法无法全面地在 RTL 设计中体现亚稳态现象,所以很难在 RTL 验证阶段有效地发现跨时钟域设计的功能错误,只有到 FPGA 验证阶段甚至流片后才能发现. 在验证初期对跨时钟设计功能验证的不足,严重影响了产品的上市时机.

收稿日期:2007-09-14;修回日期:2007-10-23
基金项目:国家 863 高技术研究发展计划(No. 2006AA010202)

本文提出一种新的面向跨时钟域设计的形式化验证方法,该方法可以在 RTL 验证阶段有效地发现跨时钟域设计的功能错误. 文献[3]中作者对亚稳态现象进行了模型化定义,本文在此工作基础上,首先提出描述亚稳态现象的 RTL 等价电路实现;然后,使用线性时序逻辑对跨时钟域设计进行设计规范描述;最后,针对跨时钟域设计的特点提出模型检验的优化方法:基于输入信号的迁移关系分组策略和基于数学归纳的优化策略. 本文实验用例采用 PKUnity863-2 号 SoC 系统芯片中的异步 FIFO 设计. 实验结果表明本文提出的方法不仅可以在 RTL 验证阶段有效地发现跨时钟域设计的功能错误,而且可以使验证时间随实验用例中寄存器数量的递增趋势从近似指数级的增长减小到近似多项式级的增长,这充分体现了本文方法的实用性.

2　相关工作

2.1　形式化验证

形式化验证是使用数学推理来证明一个系统满足设计规范的方法. 形式化验证方法可分为两大类:等价性检验(Equivalence Checking)和模型检验(Model Checking). 等价性检验一般用于可测性设计、逻辑综合和物理综合等流程前后的功能一致性验证[4],而模型检验通常用于验证设计规范与 RTL 设计实现之间的功能一致性[5].

模型检验的基本思想是使用时序逻辑形式化描述设计规范,利用有限状态机表示电路实现的状态及状态间的迁移关系,使用二叉判定图(Binary Decision Diagram,BDD)表示上述状态机,通过遍历 BDD 来检验电路实现是否符合设计规范,如果不符合则给出反例[6].

本文采用模型检验技术进行跨时钟域设计的功能验证,为缓解空间爆炸问题,本文提出基于输入信号的迁移关系分组策略和基于数学归纳的优化策略. 文献[7]中提出了一种基于状态位变化的迁移关系分组策略,相比于该方法本文提出的基于输入信号的迁移关系分组策略更易于验证者进行实现. 文献[8]运用归纳法对乘法器电路进行了 BDD 化简,本文将归纳法运用到跨时钟域设计的格雷码指针递增电路的验证中.

2.2　跨时钟域设计的验证方法

文献[9]中分析了导致跨时钟域设计功能错误的典型电路结构并给出了解决方案,但并没有提出系统的验证方法. 在文献[10]中作者提出了 MTE 模型来描述由于时序违例导致的功能错误,并定义了可以用于模拟验证的功能覆盖率,但 MTE 模型并没有区分建立或保持时间违例,与亚稳态现象的实际影响并非完全等价. 文献[11]对跨时钟域设计采用了形式化验证方法,提出了描述亚稳态现象的电路模型,但该模型对 CDC 信号仅增加了一个时钟周期的延时,并不能完全体现亚稳态现象的实际影响. 在文献[12]中,作者对 CDC 信号同步器的设计规范进行了时序逻辑描述,但并没有引入亚稳态现象的等价电路,并且同步器的结构过于简单,不适用于实际系统芯片中跨时钟域设计的功能验证.

文献[3]对亚稳态现象进行了模型化定义,并提出了适用于模拟验证的 CDC 覆盖率. 本文在此基础上,提出跨时钟域设计的形式化验证方法.

3　亚稳态现象及其等价电路实现

有效验证跨时钟域设计的前提条件是在 RTL 验证流程中准确描述亚稳态现象. 本节将首先介绍亚稳态现象和 CDC 设计中功能错误的本质原因;然后定义 5 种 CDC 状态[3],并分析传统验证方法难以全面发现跨时钟域设计错误的原因;最后用 RTL 描述亚稳态现象的等价电路实现.

3.1　亚稳态现象

考虑图 1 中的 CDC 信号 $R1$,它是 CLKA 时钟域的寄存器 FF1 的输出信号,被 CLKB 时钟域的寄存器 FF2 采样. CLKA 和 CLKB 是两个异步时钟,因此 $R1$ 可能在 FF2 寄存器的建立时间或保持时间内变化. 如果 $R1$ 在 FF2 的建立时间或保持时间内变化,则 FF2 将进入亚稳定状态. 虽然 FF2 的输出信号 $R2$ 会最终稳定到逻辑 0 或逻辑 1,但结果不可预测,这种现象被称为 CDC 信号的亚稳态现象.

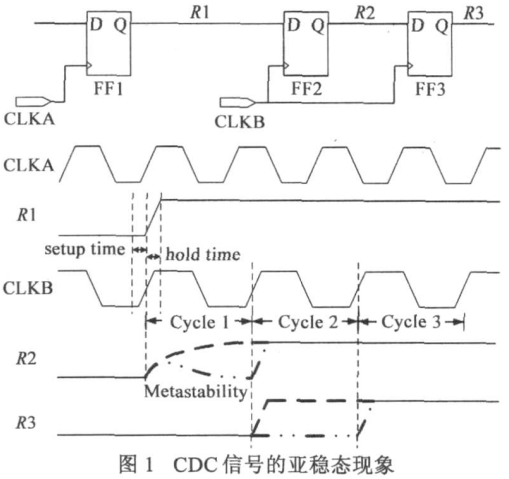


图 1　CDC 信号的亚稳态现象

虽然同步器可以消除亚稳态现象,但其输出体现输入变化的确切时钟周期仍然不可预测. 如图 1 中两级寄存器 FF2 和 FF3 组成的同步器,其输出信号 $R3$ 虽然不存在亚稳态现象,但 $R3$ 体现 $R1$ 变化的时钟周期可能在 Cycle 2 也可能在 Cycle 3[13]. 这种不确定性是跨时钟域设计中功能错误的本质原因.

3.2　CDC 状态

一个 CDC 信号相对于采样寄存器的时钟变化时刻

有以下三种情况:(1) 在建立时间内;(2) 在保持时间内;(3) 在除了建立和保持时间以外的时间内. 如果 CDC 信号在采样寄存器的建立时间或保持时间内变化,则采样寄存器在本周期可能采样到或采样不到该信号的变化. 由此可以针对 CDC 信号的采样结果定义以下 5 种 CDC 状态:

定义 1 CDC 状态

(1) CDC 信号在寄存器的建立时间内变化,寄存器采样到该变化;

(2) CDC 信号在寄存器的建立时间内变化,寄存器没有采样到该变化;

(3) CDC 信号在寄存器的保持时间内变化,寄存器采样到该变化;

(4) CDC 信号在寄存器的保持时间内变化,寄存器没有采样到该变化;

(5) CDC 信号在除建立和保持时间以外的时间内变化,寄存器采样到该变化.

在普通的 RTL 验证方法中,只有时钟沿之前的变化才能被寄存器采样到,所以普通方法只能描述 CDC 状态(1)、(4) 和(5);文献[10]提出了 MTE 模型,但其并没有区分 CDC 状态(2) 和(3);文献[11]提出的方法并不能体现 CDC 状态(3). 因此,传统验证方法无法在 RTL 验证流程中全面体现亚稳态现象.

3.3 亚稳态现象的等价电路实现

为了能够在 RTL 验证流程中全面描述上述 5 种 CDC 状态,本文提出如图 2 所示的电路结构.

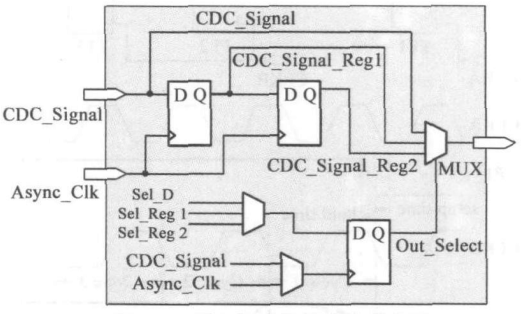


图 2 亚稳态现象的等价电路实现

当输入的 CDC 信号 CDC_Signal 在采样寄存器的建立时间内变化时,输出选择信号 Out_Select 由 Async_Clk 异步时钟寄存生成,输出选择器 MUX 将选择 CDC_Signal_Reg1 或 CDC_Signal_Reg2 信号,以实现 CDC 状态(1) 和(2) 的效果. 如果 CDC_Signal 在采样寄存器的保持时间内变化,则 Out_Select 信号由 CDC_Signal 信号寄存生成,输出选择器 MUX 将选择 CDC_Signal 或 CDC_Signal_Reg1 信号,以实现 CDC 状态(3) 和(4) 的效果. 其他情况则选择 CDC_Signal_Reg1 以实现 CDC 状态(5) 的效果.

在进行本文提出的验证方法之前,需要将所有跨时钟域路径的终点寄存器(如图 1 中的 *FF*2) 替换为上述亚稳态现象的等价电路实现.

4 跨时钟域设计的设计规范描述

在建立了亚稳态现象的等价电路实现之后,本节将讨论跨时钟域设计的设计规范描述方法. 由于 SoC 系统芯片中通常采用异步 FIFO 进行跨时钟域的数据传输,而且异步 FIFO 中包括了同步器、格雷码和二进制编码转换逻辑、指针递增逻辑、空满信号产生逻辑等跨时钟域设计中典型的电路结构,所以本文以异步 FIFO 为例,讨论跨时钟域设计的设计规范描述方法.

4.1 跨时钟域设计的电路特性

在模型检验中,设计规范的描述被称为电路的特性(Property). 通常从安全性(Safety)、存活性(Liveness) 和公平性(Fairness) 三方面描述电路特性. 安全性是指电路始终保持的状态;存活性是指电路最终会达到的状态;公平性是指电路最终会处于某些状态的循环之中,公平性一般仅用于仲裁器的特性描述.

异步 FIFO 主要包括写操作控制(Write Control)、读操作控制(Read Control) 和存储体(SRAM) 三部分电路(如图 3 所示). 其输入输出信号主要包括三类:(1) 时钟信号:读时钟(rclk) 和写时钟(wclk);(2) 控制信号:FIFO 空(empty)、FIFO 满(full)、读使能(ren) 和写使能(wen);(3) 数据信号:读数据(rdata) 和写数据(wdata). 读写操作控制分别是读写两个时钟域的逻辑,其中包括格雷码指针递增和空满信号产生等逻辑. 跨时钟域传输的信号是格雷码编码的读指针(rptr) 和写指针(wptr).

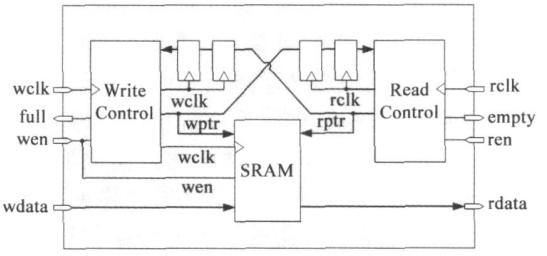


图 3 异步 FIFO 结构图

根据异步 FIFO 的特点,本文针对控制信号和电路内部表征电路状态的寄存器,从安全性和存活性两方面制定电路特性. 对于空满信号,安全性有两个:首先 empty 和 full 不能同时为真;其次,当 FIFO 为空时,写指针经过跨时钟域传输后和读控制逻辑生成的 empty 一定为真,当 FIFO 满时,读指针经过跨时钟域传输后和写控制逻辑生成的 full 一定为真. 由于经过同步器传输的指针信号有不确定的延时(如 3.1 小节所述),所以空满信号的存活性为:当 empty 为真且 FIFO 非空时,empty 最终将会撤消;当 full 为真且 FIFO 非满时,full 最终将会撤消. 对于表征电路状态的格雷码读写指针,需要检查的

安全性是:每次变化前后指针向量的汉明距离(Hamming Distance)为 1,即变化前后相邻的两个 n 位指针向量,有且仅有一位不同.

4.2　电路特性的形式化描述

在制定了电路特性以后,本节采用 LTL(Linear Temporal Logic)线性时序逻辑进行电路特性的形式化表述. 一个 LTL 公式由两部分组成:(1)状态布尔函数(State Formulas),用来表示电路中变量的布尔关系;(2)路径时序运算符(Path Formulas),用来表示布尔函数在路径上的时序逻辑.

最基本的路径时序运算符有:U(Until)和 X(neXt),其他时序运算符可由 U 和 X 组合而成. 定义状态转换路径 $\pi = s_1 \rightarrow s_2 \rightarrow \cdots \rightarrow s_i \rightarrow \cdots$,其中 s_i 为电路状态,$\rightarrow$为状态转换关系. 假设 s_1 是当前状态,如果 f 和 g 是状态布尔函数,则在路径 π 上的 LTL 公式 Xf 为真当且仅当 f 在状态 s_2 为真,f U g 为真当且仅当存在自然数 $k \geq 1$,任取 j 在 $1 \leq j < k$,使得 f 在状态 s_j 为真,并且 g 在状态 s_k 为真. 如果 f 和 g 是时序逻辑,则定义 π_j 为 π 中以状态 s_j 为起点的子路径,Xf 为真当且仅当 f 在路径 π_2 上为真,f U g 为真当且仅当存在自然数 $k \geq 1$,任取 j 在 $1 \leq j < k$,使得 f 在路径 π_j 上为真,并且 g 在路径 π_k 上为真.

LTL 公式的组成遵循以下原则:状态的布尔函数为 LTL 公式;如果 f 和 g 是 LTL 公式,则 Xf 和 f U g 也是 LTL 公式. 其他常用的路径时序运算符 F(Future)、G(Global)和 GF(Always Eventually)均可以用 U 和 X 按照上述原则组合而成,例如:

$$\mathrm{F}g = (TRUE\ \mathrm{U}\ g)$$
$$\mathrm{G}g = \sim(\mathrm{F}\sim g)$$
$$\mathrm{GF}g = G(\mathrm{F}g)$$

利用 LTL 线性时序逻辑,对 4.1 小节描述的异步 FIFO 电路特性的形式化描述如下:

G(∼(empty & full))
G(FIFO 空 →empty)
G(FIFO 满 →full)
G((empty & FIFO 非空) →F(∼empty))
G((full & FIFO 非满) →F(∼full))
G(Hamming_Distance(wptr,wptr_reg) = 1)
G(Hamming_Distance(rptr,rptr_reg) = 1)

其中 Hamming_Distance()函数返回两个输入变量的汉明距离,wptr_reg/rptr_reg 分别为变化前的 wptr/rptr 值.

5　模型检验中的优化方法

在制定了电路特性以后,为了使跨时钟域设计的模型检验方法更为实用,本节将提出两种缓解空间爆炸问题的优化方法:基于输入信号的迁移关系分组策略和基于数学归纳的优化策略.

5.1　基于输入信号的迁移关系分组策略

在模型检验中,电路实现的状态转换关系被映射为有限自动机,它可以由五元组$\langle Q, \Sigma, \delta, q_0, F\rangle$表示. 其中 Q 表示状态集合;Σ表示输入变量取值集合;δ表示状态迁移函数,即 $\delta: Q \times \Sigma \rightarrow Q$;$q_0$ 表示初始状态;F 表示最终状态集合. 状态迁移函数 δ根据当前状态和输入取值生成下一状态:$n = \delta(p, a)$,其中 $p \in Q$ 为当前状态,$a \in \Sigma$为输入取值,$n \in Q$ 为下一状态. 在模型检验中,为使状态及其转换关系可以符号化表示,引入状态迁移的特征函数 $T(p, n, a)$,其定义如下:

$$T(p,n,a) = \begin{cases} 1, & n = \delta(p,a) \\ 0, & \text{其他情况} \end{cases} \quad (1)$$

该特征函数为 1 当且仅当输入取值、当前状态和下一状态满足状态迁移关系.

为检查是否满足相关特性,模型检验需要计算电路的可达状态空间,为此引入下一状态的特征函数 $N(n)$,其定义如下[14]:

$$N(n) = \begin{cases} 1, & \exists (p,a)(T(p,n,a) \cdot P(p) = 1) \\ 0, & \text{其他情况} \end{cases} \quad (2)$$

该特征函数为 1 当且仅当对于给定的当前状态特征函数 $P(p)$和输入取值 $a \in \Sigma$,存在满足状态迁移特征函数(1)的下一状态. 为求出电路可达状态空间,可以从初始状态 q_0 开始,对下一状态特征函数(2)进行迭代,当迭代结果不增加新的可达状态时迭代过程结束.

由此可见,对于下一状态特征函数 $N(n)$的优化有利于减少求解可达状态空间的复杂度,即有利于缓解模型检验中随电路规模增加导致的空间爆炸问题.

由于在功能验证过程中验证者比较容易根据待验证特性对某些输入信号的取值进行约束,所以本文提出基于输入变量的状态迁移特征函数的分组策略. 由于 $P(p)$与输入取值并不相关,下一状态特征函数 $N(n)$可以进行以下变换:

$$\begin{aligned} N(n) &= \exists (p,a)(T(p,n,a) \cdot P(p)) \\ &= \exists p((\exists aT(p,n,a)) \cdot P(p)) \end{aligned} \quad (3)$$

进一步对式(3)中的存在运算 $\exists aT(p,n,a)$进行余因子(cofactor)变换:

$$\exists aT(p,n,a) = \sum_{m \text{ is a minterm of } a} T_m(p,n,a) \quad (4)$$

如果存在某个输入取值的因子 m,使得状态迁移的特征函数对其余因子为 0,则可以将该余因子从上述存在运算中去除. 即:

$$T_m(p,n,a) = 0 \Rightarrow \exists aT(p,n,a) = T_{\bar{m}}(p,n,a)$$

或

$$T_{\bar{m}}(p,n,a) = 0 \Rightarrow \exists aT(p,n,a) = T_m(p,n,a)$$

基于输入信号的迁移关系分组策略的直观含义是:在模型检验过程中,验证者如果能够确定对于某个输入信号的某个取值不能引起待验证特性所对应电路状态的转移,则可以将该取值在状态迁移特征函数中去除掉,以减小为求解可达状态空间的迭代次数.

5.2 基于数学归纳的优化策略

在跨时钟域设计中,多位信号同时在跨时钟域路径上进行传输需要进行格雷码转换.其典型应用是异步 FIFO 中的格雷码指针递增电路,本文针对此类电路结构(如图 4 所示),提出基于数学归纳的优化策略.

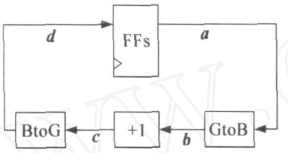


图 4 格雷码指针递增电路结构图

图 4 中 BtoG 模块为二进制向格雷码转换电路,GtoB 为格雷码向二进制转换电路,其中 a,b,c,d 均为 n 位向量. a 为格雷码指针,b 为经过 GtoB 变换后的二进制指针,c 为进行加 1 运算后的二进制指针,d 为经过 BtoG 变换后的格雷码指针.在异步 FIFO 中,格雷码指针 a 将会被传送到异步时钟域进行指针比较.格雷码指针递增的电路实现中各变量的逻辑关系表述如下:

$$a = (a_{n-1}, \cdots, a_1, a_0)$$

$$b = (b_{n-1}, \cdots, b_1, b_0) = GtoB(a) \tag{5}$$

$$= \begin{cases} b_i = a_i, & i = n-1 \\ b_i = b_{i+1} \oplus a_i, & 0 \le i < n-1 \end{cases} \tag{6}$$

$$c = (c_{n-1}, \cdots, c_1, c_0) = b + 1 \tag{7}$$

$$d = (d_{n-1}, \cdots, d_1, d_0) = BtoG(c)$$

$$= \begin{cases} d_j = c_j, & j = n-1 \\ d_j = c_{j+1} \oplus c_i, & 0 \le j < n-1 \end{cases} \tag{8}$$

该电路的待验证特性为:每次格雷码指针变换前后的汉明距离为 1,即 a 与 d 的汉明距离为 1.

本文提出的基于数学归纳的验证流程为:

首先需要验证 $n = 2$ 时该特性成立;

然后假设 $n = k (k \ge 2)$ 时该命题成立,则当 $n = k + 1$ 时,分两种情况讨论:

情况 1 如果 $a_k = d_k$,则根据式(6)和(8)有 $c_k = b_k$,可知指针在 $n \le k-1$ 位内递增变换,根据假设有此时命题成立;

情况 2 如果 $a_k \ne d_k$,则根据式(6)和(8)有 $c_k \ne b_k$,根据式(7)再分两种情况讨论:

(a) $b_k = 0$, $b_i = 1 (0 \le i \le k-1)$ 且 $c_k = 1$, $c_i = 0 (0 \le i \le k-1)$,此时根据式(6)有:$a_k = 0$, $a_{k-1} = 1$, $a_i = 0 (0 \le i \le k-2)$,再根据式(8)有:$d_k = 1$, $d_{k-1} = 1$, $d_i = 0 (0 \le i \le k-2)$,根据汉明距离定义得知此时 a 与 d 的汉明距离为 1.

(b) $b_i = 1$, $c_i = 0 (0 \le i \le k)$ 此时根据式(6)有:$a_k = 1$, $a_i = 0 (0 \le i \le k-1)$,再根据式(8)有:$d_i = 0 (0 \le i \le k)$,则此时 a 与 d 的汉明距离为 1.

由此可见,为验证上述电路的 n 位格雷码指针向量 a 与 d 的汉明距离为 1,只需验证只有最低 2 位递增时该特性成立即可.

6 实验结果

本文采用 Cadence SMV[15] 作为形式化模型检验工具,使用 LTL 线性时序逻辑对跨时钟域设计进行电路特性的描述,使用 SMV 语言进行优化方法的实现.实验硬件环境为 SUN Blade 2000 工作站,配置两个 UltraSparcIII 900MHz 处理器和 4G 物理内存,操作系统为 Solaris 8.

本文实验用例使用 PKUnity863-2 号 SoC 系统芯片内 AHB-PCI 桥接器中的异步 FIFO 设计,该设计使用 Verilog RTL 进行电路描述,电路结构如图 5 所示.其中信号含义如 4.1 和 5.2 小节所述,该 FIFO 深度和宽度可配置.

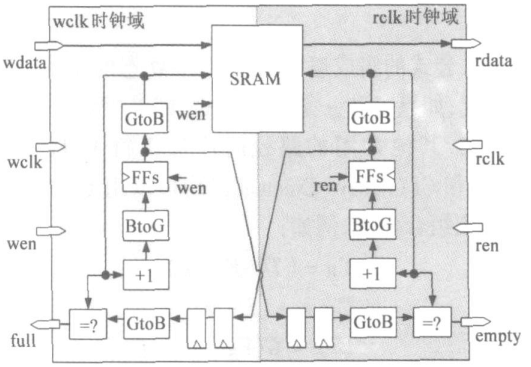


图 5 AHB-PCI 桥接器中的异步 FIFO 电路结构

实验针对不同的 FIFO 深度,按照第 4 节所述的电路特性描述设计规范,采用第 5 节的优化方法进行模型检验,对比优化前后验证时间和 BDD 节点数目的不同.

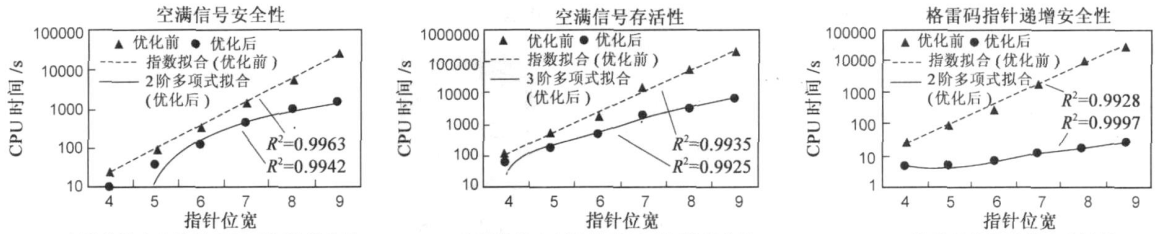
第 4 节所述的电路特性可以分为三类:空满信号的安全性、空满信号的存活性和格雷码指针递增的安全性.对于空满信号的安全性和存活性的验证,在其状态迁移关系中采用对输入读写使能信号进行分组的策略.对于格雷码指针递增的安全性验证,采用基于数学归纳的方法进行优化,将指针的高位约束为 0,验证只有最低 2 位递增时的正确性,则根据 5.2 小节可以得出格雷码指针递增的汉明距离为 1.

实验数据如表 1 所示,FIFO 深度分别被配置为 8、16、32、64、128 和 256 个表项,对应的指针宽度分别为 4、5、6、7、8 和 9 位,由于本文制定的电路特性与 FIFO 的数

据宽度无关,所以在"寄存器数量"中列出的是除去 SRAM 存储体以外的寄存器个数.表中分别对比了验证上述三类特性所占用的 CPU 时间(单位为秒)和 BDD 节点数目,BDD 节点数目直接影响了程序占用内存的大小.数据显示随指针位宽的线性增加,电路中寄存器数量也线性增加,而优化前的验证时间近似指数级增长,BDD 节点数目也迅速增加.

表 1　采用本文提出的优化方法前后,验证时间和 BDD 节点数目的对比

FIFO 深度	指针位宽	寄存器数量	优化前						优化后					
			空满信号安全性		空满信号存活性		格雷码安全性		空满信号安全性		空满信号存活性		格雷码安全性	
			Time(s)	BDD	Time(s)	BDD	Time(s)	BDD	Time(s)	BDD	Time(s)	BDD	Time(s)	BDD
8	4	69	25.7	124,791	104.4	209,719	25.6	122,715	10.4	65,576	58.2	164,184	3.9	32,058
16	5	82	95.8	257,935	487.2	550,401	86.0	225,747	35.6	113,874	150.8	375,483	4.4	45,548
32	6	95	306.6	586,956	1641.1	1,482,702	277.9	647,279	120.1	221,505	423.4	791,397	6.4	56,802
64	7	108	1271.1	1,308,547	14921.5	6,918,788	1666.2	838,661	403.3	552,931	1851.6	2,649,746	10.9	56,838
128	8	121	5116.2	1,680,122	49210.7	17,451,830	10172.6	2,957,179	904.6	585,284	3081.7	3,010,886	16.6	68,392
256	9	134	28749.4	3,461,793	181413.0	47,446,267	29677.5	4,632,820	1337.5	834,937	6677.7	6,553,395	24.8	119,317



(a)空满信号安全性的验证时间增长趋势　(b)空满信号存活性的验证时间增长趋势　(c)格雷码指针递增安全性的验证时间增长趋势

图 6　对比采用本文提出的优化方法前后,验证时间的增长趋势

图 6 中对比了采用本文提出的优化方法前后,验证时间的增长趋势.其中 R^2 是拟合趋势线的决定系数,表示拟合趋势线的估计值与对应的实际数据之间的拟合程度,决定系数 R^2 值越接近 1,拟合函数可靠性越高.图中所示的拟合趋势线选取的是 R^2 值最大的拟合趋势线.

其中采用基于输入信号迁移关系分组策略进行验证的空满信号安全性和存活性,优化前验证时间随指针宽度的递增呈近似指数级的增长(R^2 为 0.9963),而优化后验证时间随指针宽度的递增分别呈近似 2 阶多项式的增长(R^2 为 0.9942)和近似 3 阶多项式的增长(R^2 为 0.9925).对于采用基于数学归纳进行验证的格雷码指针递增安全性的优化效果也表现出同样的趋势.实验数据表明本文提出的对验证时间的优化方法可以将跨时钟域设计的模型检验时间控制在可接受的范围内.

在采用本文提出的方法对实验用例进行模型检验的过程中,发现了该设计在原有模拟验证和 FPGA 验证过程中均没有发现的两处设计错误:一个出现在空满信号的产生逻辑中,另一个出现在跨时钟域指针的同步器逻辑中.这充分说明了本文提出的方法可以在 RTL 验证阶段有效地发现跨时钟域设计的功能错误.

7　结论

跨时钟域设计被越来越多地应用到 SoC 系统芯片中,然而传统的验证方法无法在 RTL 验证阶段全面地发现跨时钟域设计的功能错误,这严重影响了产品的上市时机.为解决此问题,本文首先提出亚稳态现象的等价电路实现,用以在 RTL 验证中准确体现亚稳态现象的实际影响;然后使用线性时序逻辑对跨时钟域设计进行设计规范描述;为提高实用性,进一步提出基于输入信号的迁移关系分组策略和基于数学归纳的优化策略,以优化模型检验的时间代价.本文采用 PKUnity863-2 号 SoC 系统芯片中的异步 FIFO 作为实验用例,实验结果表明本文提出的方法不仅可以在 RTL 验证阶段有效地发现跨时钟域设计的功能错误,而且可以使验证时间随实验用例中寄存器数量的递增趋势从近似指数级的增长减小到近似多项式级的增长.

参考文献:

[1] Intel Corporation. Intel CE 2110 media processor[DB/OL]. http://www.intelconsumerelectronics.com/Technologies/CE2110.aspx,2007-04-17/2007-08-07.

[2] Michael Keating, Pierre Bricaud. Reuse Methodology Manual for System-on-a-Chip Designs (Third Edition)[M]. Boston:. Kluwer Academic Publisher,2002. 239 - 264.

[3] Feng Yi, Zhou Zheng, Tong Dong, Cheng Xu. Clock domain crossing fault model and coverage metrics for validation of SoC design[A]. Design, Automation & Test in Europe Conference &

Exhibition[C]. San Jose: EDA Consortium, 2007. 1385 - 1390.

[4] 严晓浪,郑飞君,葛海通,杨军. 结合二叉判决图和布尔可满足性的等价性验证算法[J]. 电子学报, 2004, 32(8): 1233 - 1235.
Yan Xiaolang, Zheng Feijun, Ge Haitong, Yang Jun. Combining binary decision diagrams and boolean satisfiability for equivalence checking[J]. Acta Electronica Sinica, 2004, 32(8): 1233 - 1235. (in Chinese)

[5] Kenneth L McMillan. Symbolic Model Checking: an Approach to the State Explosion Problem[D]. Pittsburgh: Carnegie Mellon University, 1992.

[6] 林惠民,张文辉. 模型检测:理论、方法与应用[J]. 电子学报, 2002, 30(12A): 1907 - 1912.
Lin Huimin, Zhang Wenhui. Model checking: theories, techniques and applications[J]. Acta Electronica Sinica, 2002, 30(12A): 1907 - 1912. (in Chinese)

[7] 邵明,李光辉,李晓维. 模型检验中迁移关系的分组策略[J]. 计算机辅助设计与图形学学报, 2003, 15(9): 1101 - 1104.
Shao Ming, Li Guanghui, Li Xiaowei. Strategy to group partitioned transition relationship in model checking[J]. Journal of Computer-Aided Design & Computer Graphics, 2003, 15(9): 1101 - 1104. (in Chinese)

[8] Ying-Tsai Chang, Kwang-Ting (Tim) Cheng. Induction based gate level verification of multipliers[A]. Proceedings of the 2001 IEEE/ACM International Conference on Computer Aided Design[C]. Piscataway: IEEE Press, 2001. 190 - 193.

[9] Ran Ginosar. Fourteen ways to fool your synchronizer[A]. Proceedings of Asynchronous Circuits and Systems[C]. Washington: IEEE Computer Society, 2003. 89 - 91.

[10] Q Zhang, IG Harris. A validation fault model for timing induced functional errors[A]. International Test Conference[C]. Washington: IEEE Computer Society, 2001. 813 - 820.

[11] Tai Ly, Neil Hand, Chris Ka-kei Kwok. Formally verifying clock domain crossing jitter using assertion-based verification[A]. Design and Verification Conference[C]. San Jose: EDA Direct, 2004. 1 - 5.

[12] Tsachy Kapschitz, Ran Ginosar. Formal verification of synchronizers[A]. Proceedings of Correct Hardware Design and Verification Methods[C]. New York: Springer, 2005. 359 - 362.

[13] Charles Dike, Edward Burton. Miller and noise effects in a synchronizing flip-flop[J]. IEEE Journal of Solid-State Circuits, 1999, 34(6): 849 - 855.

[14] William K Lam. Hardware Design Verification: Simulation and Formal Method-Based Approaches[M]. Indiana: Prentice Hall PTR, 2005.

[15] Kenneth L McMillan. Getting started with SMV[DB/OL]. http://www.kenmcmil.com, 1999-03-23/2007-08-07.

作者简介:

冯 毅 男,1981 年生于北京,北京大学计算机系博士研究生. 主要研究方向为软硬件协同设计、系统芯片的设计与验证.
E-mail: fengyi@mprc.pku.edu.cn

易江芳 女,1977 年生于四川什邡,北京大学计算机系博士. 主要研究方向为软硬件协同设计、芯片验证和测试自动生成.

刘 丹 女,1983 年生于湖南长沙,北京大学计算机系博士研究生. 主要研究方向为片上通信结构的设计与验证.

佟 冬 男,1971 年生于吉林长春,北京大学计算机系副教授. 主要研究方向为高性能微处理器、系统芯片、体系结构等.

程 旭 男,1967 年生于新疆乌鲁木齐,北京大学计算机系教授,博士生导师. 主要研究方向为高性能微处理器、系统芯片、嵌入式系统、指令级并行、优化编译、软硬件协同设计等.