文章编号:1671-4598(2022)04-0035-05 DOI:10.16526/j.cnki.11—4762/tp.2022.04.006 中图分类号:TN402 文献标识码:A

基于形式验证的多周期路径检测技术

朱秋岩
(北京航天自动控制研究所，北京 100854)

摘要：多周期路径是将复杂电路运算拆分在多个时钟周期完成，从而提高电路总体运行频率的一种方法；在设计和验证中，多周期路径约束错误会导致设计迭代反复和验证误报；文章对多周期路径的产生机理和设计验证中常见的问题进行分类分析，提出一种用静态时序分析和形式验证结合来查找设计中的多周期路径的方法，首先通过静态时序分析，查找出时序违例的路径，针对这些路径，插入设计的检测电路，检测电路主要通过检测目的触发器采样控制信号有效时间，来判断该路径是否为多周期路径；采用基于断言的形式验证，用自动化的手段检测多周期路径；实践结果表明，该方法针对两种时钟下的多周期路径，能够100%准确地检测出违例的多周期路径，避免多周期路径错误约束，省略人工分析和动态仿真确认多周期路径环节。

关键词：SOC验证；时序分析；形式验证；多周期路径；断言

Formal Verification Based on Detection Technology of Multicycle Path

ZHU Qiuyan
(Beijing Institute of Computer Technology and Application, Beijing 100854, China)

Abstract: A multicycle path is a way to split complex circuit operations into multiple clock cycles to improve the circuit clock frequency. The error constraint of multicycle path may cause design iterations and false positives in design and verification. In this paper, the generation mechanism for multicycle path and the common problems in design and verification are classified and analyzed. A method of finding multicycle paths is presented by combining formal verification with static timing analysis. Firstly, through static time sequence analysis, the paths of time sequence violation are found out. Then, the designed detection circuit is inserted in these paths. By detecting the valid time for register sampling control signal, whether the path is a multicycle path can be determined. The detection circuit is validated in the form of assertions, and multicycle paths are detected by automated means. The results show that the proposed method can effectively detect all error multicycle paths within two clocks, and it avoids the error constraint of multicycle path, and omits the manual analysis to confirm the multicycle paths.

Keywords: SOC verification; timing analysis; formal verification; multicycle path; assertion

0 引言

随着集成电路复杂度和规模的日益增加，芯片集成度越来越高，时钟频率也不断提高。因此，电路的时序分析和优化在集成电路设计中也越来越关键。其中，多周期路径约束作为修正建立和保持时间违例的方法，被广泛应用到芯片设计和验证中[1]。

在默认的同步电路静态时序分析中，都是按照单周期计算数据路径的建立和保持时间，但是往往存在这样的情况：一些数据不需要在下一个周期就稳定下来，可能在数据发送后的几个时钟周期之后才被使用；针对这种情况，时序分析工具无法猜度出来[2]，时序约束工具会按照单周期路径检查方法执行，虚报时序违例。多周期路径约束是用来解决这个问题的。多周期路径约束是指电路中信号从寄存器A传递到寄存器B的输入端，允许延迟一个以上的CLK时钟周期的路径约束。

在以往时序分析中，这种虚报时序违例造成其他布局布线资源侵占和设计迭代反复[3]。提出了多周期路径施加约束的方法，但是对于因多周期路径约束错误导致的时序违例，需要验证人员通过分析设计意图和动态仿真测试的方法，逐一确认是否为虚报，这样需要验证人员对所有的电路内部细节功能和输入输出情况分析和仿真，提高了验证难度，也极大降低验证效率，增加了验证周期[1]。虽然在设计中添加断言来提高多周期路径的检测效率，但是仍然采用动态仿真测试的方法确认多周期路径[4]。采用D算法分析了组合逻辑电路的敏感路径，却没有准确找出多周期路径[5]。采用智能的静态时序分析工具添加约束，可以降低多周期路径误报，但是无法100%准确的消除多周期路径误报[6]。采用声明虚假路径的办法，消除误报，但是这种过于宽松的约束会造成时序违例的漏报[7-8]。

本文通过分析多周期路径的产生机理和设计验证中的常见问题，对多周期路径进行分类与归纳，提出一种基于形式验证和静态时序分析相结合的方法，用纯静态的方式，无需深入分析和动态仿真电路功能，即可检测设计中的多周期路径，用于静态时序分析约束。

收稿日期:2021-09-02； **修回日期**:2021-11-08。
作者简介:朱秋岩(1986-)，女，河南濮阳人，硕士研究生，高级工程师，主要从事FPGA设计与验证技术方向的研究。
引用格式:朱秋岩.基于形式验证的多周期路径检测技术[J].计算机测量与控制,2022,30(4):35-39,97.

1 多周期路径的分类

多周期路径根据应用场景的不同，可以分为相同时钟的多周期路径和不同时钟间的多周期路径。

相同时钟间的多周期路径，也是最常见的多周期路径，源触发器和目的触发器使用同一个时钟信号，但源触发器与目的触发器之间的组合逻辑延迟大于一个时钟周期，如图 1 所示。其中源触发器和目的触发器之间的慢速组合逻辑延迟 2 个或多个时钟周期，在数据到达目的触发器之前，目的触发器使能 ENA 端应维持无效，目的触发器输出端 Q 的值只有在数据到达后才会更新。

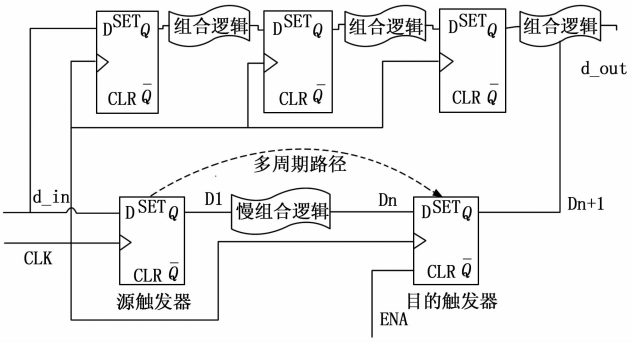

图 1 同一时钟间多周期路径示意图

不同时钟之间的多周期路径如图 2 所示。源触发器和目的触发器由不同的时钟信号驱动，因为静态时序分析主要针对同源时钟分析，所以这里不同的时钟为同源的、具有固定相位关系的时钟，根据其时钟频率关系的不同又可以分为快时钟到慢时钟的多周期路径和慢时钟到快时钟的多周期路径两种。

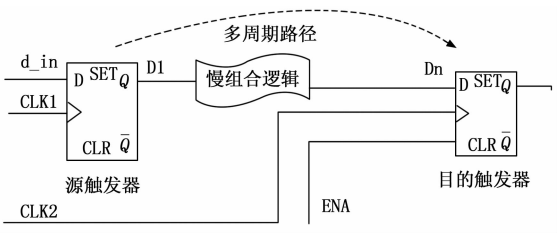

图 2 不同时钟间多周期路径示意图

2 多周期路径的时序分析

静态时序分析的对象包括：触发器和触发器之间的路径、I/O 之间、I/O 和触发器之间的路径、异步复位和触发器之间的路径。由于时序分析是针对时钟驱动电路进行的，所以分析的对象一定是“触发器－触发器”对。在分析涉及 I/O 的时序关系对时，看似缺少一个触发器分析对象，其实是穿过 FPGA（field-programmable gate array）的 I/O 引脚，在 FPGA 外部虚拟了一个触发器作为分析对象。所以，静态时序分析的所有类型的路径，都可以用“触发器－触发器”的路径分析方法表示。

2.1 相同时钟间的多周期路径时序分析

根据对多周期路径的分类，相同时钟间的多周期路径时序分析如图 3 所示，不设置多周期路径时，默认的建立时间路径 setup 设置为 1 个时钟周期，CLK1 信号 Tx 时刻发生翻转，即需在 $Tx+1$ 处检查 CLK1 时钟域信号的建立保持时间（虚线为单周期路径 setup 和 hold 时间要求），如果将该路径设置为 setup 为 2，hold 为 1 的多周期路径，则在 $Tx+2$ 时刻检查 setup 时间，setup 和 hold 时间均放宽松 1 个时钟周期（实线为多周期路径 setup 和 hold 时间要求）。

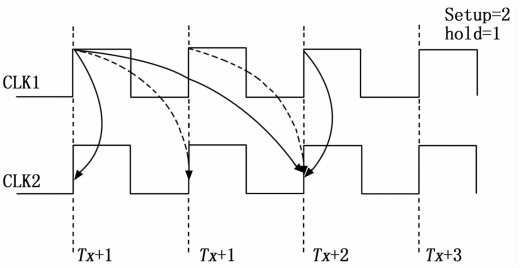

图 3 相同时钟间多周期路径时序分析图

2.2 不同时钟间的多周期路径时序分析

不同时钟间的多周期路径，从慢时钟到快时钟的多周期路径时序分析如图 4 所示，不设置多周期路径时，CLK1 时钟域信号 Tx 时刻发生翻转，虽然 Tx 到 $Tx+1$ 不满足一个时钟周期，但是分析工具为了方便，仍将 setup 定为 1 个时钟周期，即在 $Tx+1$ 处检查 CLK1 时钟域信号的建立保持时间（虚线为单周期路径 setup 时间要求），如果将该路径设置为 setup 为 2，hold 为 1 的多周期路径，则在 $Tx+2$ 时刻采样有效数据，setup 和 hold 时间均放宽松 1 个时钟周期（实线为多周期路径 setup 和 hold 时间要求）。

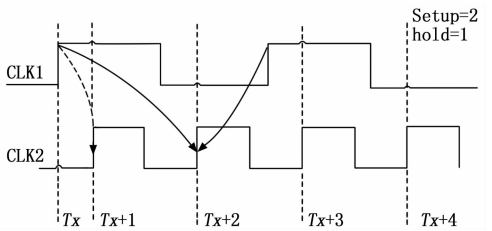

图 4 慢时钟到快时钟间多周期路径时序分析图

从快时钟到慢时钟的多周期路径时序分析如图 5 所示，不设置多周期路径时，CLK1 时钟域信号 Tx 时刻发生翻转，在 $Tx+1$ 处检查 CLK1 时钟域信号的建立保持时间，如果将该路径设置为 setup 为 2，hold 为 1 的多周期路径，则在 $Tx+2$ 时刻采样有效数据，setup 和 hold 时间均放宽松 1 个时钟周期（实线为多周期路径 setup 和 hold 时间要求）。

I/O 之间和 I/O 到触发器之间，可以等效为不同时钟间的多周期路径，时序分析与不同时钟间的多周期路径相同。

3 多周期路径检测

本文采用一种用静态时序分析和形式验证结合来查找设计中的多周期路径的方法，该方法先用静态时序分析的方法查找出违例路径，然后分析违例路径目的触发器时能

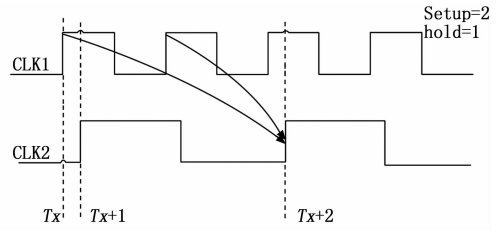

图 5　快时钟到慢时钟间的多周期路径时序分析图

端，通过检测目的触发器使能控制信号有效时间来判断该路径是否为多周期路径。检测流程如图 6 所示。

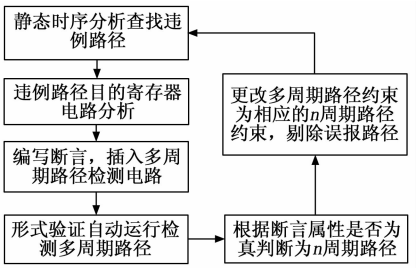

图 6　多周期路径检测流程

3.1　静态时序分析查找多周期路径

通过对不同类型单周期路径和多周期路径的静态时序分析可知，如果静态时序分析时，不设置多周期路径，实际多周期路径电路时序分析约束错误，会产生建立时间或保持时间违例的误报，所以，验证人员需要查找设计中的多周期路径，设置正确的约束，使静态时序分析结果准确无误。

首先，通过使用静态时序分析，查找出时序违例的路径（不产生违例的多周期路径不需要关注，因为不会导致时序分析违例误报）[9]，而这些路径包括单周期路径和多周期路径，单周期路径是实际真正的违例电路，多周期路径是需要检测和重新设置的[10]。传统的方法是通过动态仿真测试的方法确认这些路径哪些为多周期路径，但是动态仿真测试需要人工分析和确认，花费大量时间和精力。

3.2　形式验证检测多周期路径

本文在静态时序分析结果的基础上，设计了一种多周期路径检测电路，插入需要检测的路径，采用基于断言的形式验证，用自动化的手段检测多周期路径。形式验证技术用时态逻辑来描述设计意图，通过有效的搜索方法来检查给定的系统是否满足设计意图，将使用数学推理来验证设计意图在 RTL（register transfer level）实现中是否得以贯彻。形式验证是穷尽式数学技术，能够从算法上穷尽检查所有随时间可能变化的输入值，没有必要考虑如何设计激励或创建多种条件来实现较高的可覆盖率和可控性[11]，使多周期路径的查找更加快速可靠。

通过同一时钟间多周期路径电路图 1 和时序分析图 3 可知，如果源触发器和目的触发器之间存在多周期路径，目的触发器使能信号 ENA 可以利用计数器、移位寄存器及状态机等方法实现对目的触发器捕获周期的控制，最终表现为 ENA 在 $Tx+1$ 时刻应维持无效，如果是 2 周期路径，则 ENA 受控制，在 $Tx+2$ 时刻有效。所以，可以通过判断 ENA 的有效时刻来判断多周期路径，在图 3 的 $Tx+1$、$Tx+2$ 时刻处检查 ENA 的有效值，可以检测该路径是否为 2 周期路径。根据以上分析，设计的检测电路如图 7 所示，在被测电路出现违例的路径处插入检测电路，如果输入信号 d_in 在 Tx 时刻发生变化，由 0－>1，则用 D1 处信号作为时钟，可在 $Tx+1$ 时刻检测 ENA，期望结果为 0，说明 ENA 在 $Tx+1$ 时刻为无效，D2 处信号作为时钟，可在 $Tx+2$ 时刻检测 ENA，期望结果为 1，说明 ENA 在 $Tx+2$ 处为有效，检测结果通过组合逻辑输出为 CHECK_OUT[12]。

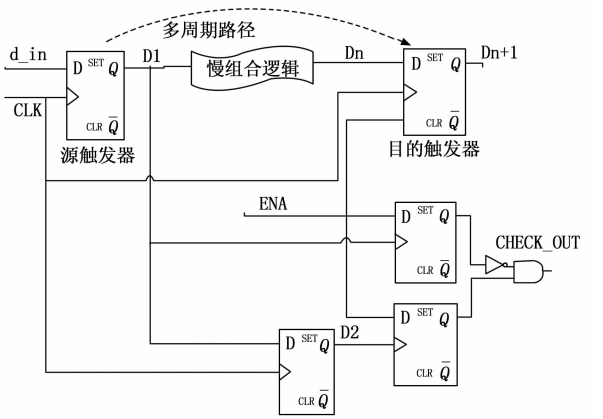

图 7　同一时钟间多周期路径检测电路

根据图 7 检测电路设计，用断言描述该属性如下所示[13]：

```
property Check_clk_Multi_cycle_2;
@(posedge Clk)
rose(d_in)|－> 2 rose(ENA);
endproperty
Sig_T:assert property(Check_clk_Multi_cycle_2);
```

如果断言属性如果为真，则该路径为 2 周期路径。依照此方法类推，如果 $Tx+1$、$Tx+2$ 时刻检查 ENA 无效，$Tx+3$ 时刻检查 ENA 有效，则可检测 3 周期路径。

慢时钟到快时钟多周期路径电路图 2 和时序分析图 4 所示，以 2 周期路径为例，最终表现为使能端 ENA 在图 4 的 $Tx+1$ 时刻应维持无效，$Tx+2$ 时刻有效，通过判断 ENA 有效时刻，来判断是否为多周期路径。但是由于源触发器和目的触发器使用时钟不同，所以在设计中插入检测电路不同，慢时钟到快时钟多周期路径检测电路如图 8 所示，如果要在图 4 的 $Tx+1$ 时刻检测 ENA 是否有效，则用输入 d_in 作为触发器 A 的使能信号，用 d_in 有效后的 CLK2 的第一个时钟沿，检测 ENA，期望结果为 0，说明 ENA 在 $Tx+1$ 时刻为无效。将 d_in 用 CLK2 作一级寄存后输出 D2，D2 信号上升沿即为 $Tx+2$ 时刻，用 D2 信号作为时钟，触发器 B 可在 $Tx+2$ 时刻检测 ENA，期望结果为 1，说明 ENA 在 $Tx+2$ 处为有效。

根据图 8 检测电路设计，用断言属性描述该行为如下所示：

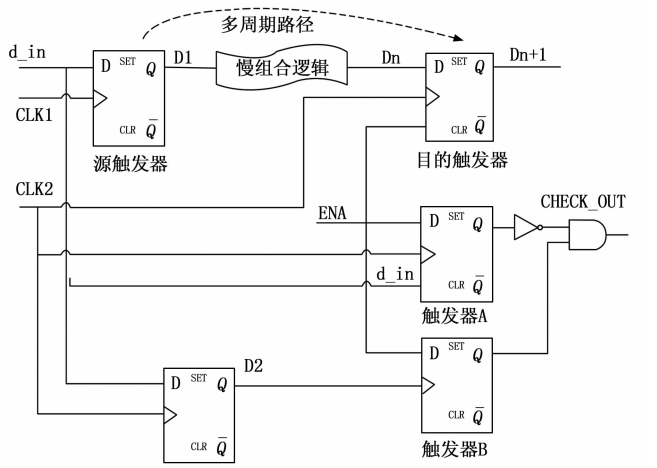

图 8 慢时钟到快时钟间多周期路径检测电路

```
property Check_clk1clk2_Multi_cycle_2;
@(posedge Clk2)
d_in|->stable(ENA)  1 rose(ENA);
endproperty
Sig_T:assert property(Check_clk1clk2_Multi_cycle_2);
```

快时钟到慢时钟多周期路径电路图 2 和时序分析图 5 所示，以 2 周期路径为例，最终表现为 ENA 在图 5 的 $Tx+1$ 时刻应维持无效，$Tx+2$ 时刻有效，检查原理与快时钟到慢时钟多周期路径检查原理一样，如果要在图 5 的 $Tx+1$ 时刻检测 ENA 是否有效，则用输入 d _ in 作为使能信号，用 d _ in 有效后的 CLK2 的第一个时钟沿，检测 ENA，期望结果为 0，说明 ENA 在 $Tx+1$ 时刻为无效。将 d _ in 用 CLK2 作一级寄存后输出 D2，D2 信号上升沿即为 $Tx+2$ 时刻，用 D2 信号作为时钟，可在 $Tx+2$ 时刻检测 ENA，期望结果为 1，说明 ENA 在 $Tx+2$ 处为有效。分析可知，快时钟到慢时钟多周期路径检测电路与图 7 相同，断言属性描述也与慢时钟到快时钟相同。

4 实验验证

本文采用 Synopys 公司的 Primetime 静态时序分析工具，用以查找时序分析时出现的违例路径。采用 Candance 公司的 Jasper 作为形式化验证工具，Jasper 采用了高性能和大规模的形式验证技术，能够穷尽地验证模块是否满足断言要求。Jasper 使用数学算法，不需要使用仿真测试平台或激励。

1）实验被测电路为相同时钟间多周期路径电路[14-15]，用 Verilog HDL 语言描述如下：

```
always@(posedge clk1)
begin
in1<=in;
end
assign in2=~in1;
assign in4=in2+in3;
assign in6=~in4+in5;
always@(posedge clk1)
begin
if(in1==0&&in==1)
counter<=2'b11;
else if(counter! =2'b00)
begin
counter<=counter-2'b01;
if(counter==2'b10)
ENA<=1;
end
end
always@(posedge clk1)
if(~ENA)
out<=0;
else
out<=in6;
```

选用器件为 Xilinx 的 xc3s50-5-pq208，使用 ISE 综合工具综合后 RTL 级电路如图 9 所示[16]，采用静态时序分析工具违例结果如表 1 所示[17-18]，静态时序分析工具显示在触发器 IN 和触发器 OUT 间出现 setup 时间违例，建立时间余量为-0.039 ns。

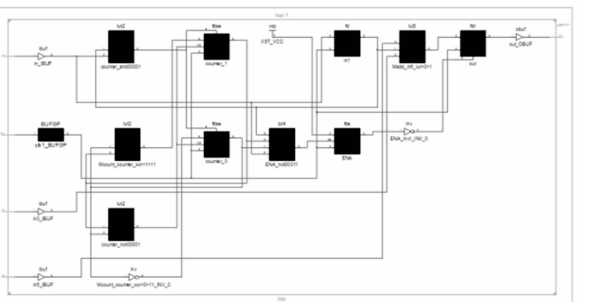

图 9 相同时钟被测电路 1

表 1 相同时钟静态时序分析违例结果

Constraint	Check	Worst Case SlackBest Case	Best Case Achievable	Worst
* TS_clk1=PERIOD TIMEGRP "clk1" 1.5 ns HI	SETUP	-0.039ns	1.539ns	1
	HOLD	0.845ns	—	0

通过 Jasper 形式化验证，利用断言检测同时钟下触发器 IN 到触发器 OUT 是否为多周期路径。

```
property Check_Sameclk_Multi_cycle_3;
@(posedge Clk)
rose(d_in)|-> 3 rose(ENA);
endproperty
Sig_T:assert property(Check_Sameclk_Multi_cycle_3);
```

形式验证结果为真，该路径为 3 周期路径。

2）实验被测电路为不同时钟多周期路径电路[19-20]，用 Verilog HDL 语言描述如下：

```
always@(posedge clk3)
begin
in1<=in;
```

```
end
assign in2=~in1;
assign in4=in2+in3;
assign in6=~in4+in5;
always@(posedge clk3)
begin
if(in1==0&&in==1)
counter<=2'b11;
else if(counter! =2'b00)
begin
counter<=counter-2'b01;
if(counter==2'b01)
ENA<=1;
end
end
always@(posedge clk2)
if(~ENA)
out<=0;
else
out<=in6;
clk clk_inst(
.CLKIN_IN(clk),
.RST_IN(1'b0),
.CLKDV_OUT(clk2),
.CLKIN_IBUFG_OUT(clk3),
.CLK0_OUT(clk1),
.LOCKED_OUT(lock));
```

选用器件仍为 Xilinx 的 xc3s50-5-pq208，使用 ISE 综合工具综合后 RTL 级电路如图 10 所示，采用静态时序分析工具违例结果如表 2 所示，静态时序分析工具显示 clk 到 CLKDV _ OUT 触发器建立时间违例，建立时间余量为－2.793 ns。

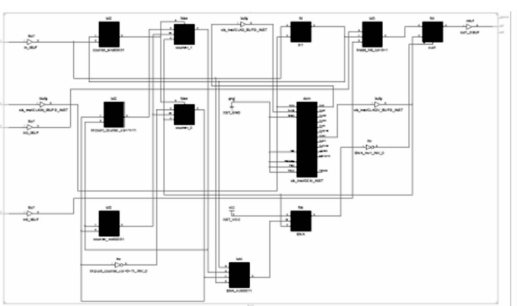

图 10　不同时钟被测电路 2

表 2　不同时钟静态时序分析违例结果

Constraint	Check	Worst Case SlackBest Case	Best Case Achievable	Worst
* TS _ clk _ inst _ CLKDV _ BUF = PERIOD TIMEGRP" clk _ inst _ CLKDV _ BUF" TS _ clk * 2 PHASE 0.046875 ns HIGH 50%	SET UP	－2.793 ns	740.608 ns	1
	HOLD	2.072 ns	—	0

通过 Jasper 形式化验证，利用断言检测不同时钟下触发器 IN 到触发器 OUT 是否为多周期路径。

```
property Check_clk1clk2_Multi_cycle_2;
@(posedge Clk2)
d_in|->stable(ENA)  1 rose(ENA);
endproperty
Sig_T:assert property(Check_clk1clk2_Multi_cycle_2);
```

形式验证结果为真，该路径为 2 周期路径。

通过实验结果表明，本文提出的多周期路径查找方法，能够准确检测出多周期路径的存在，避免静态时序分析误报问题。

5　结束语

文中对多周期路径进行了系统的分析研究，按照多周期路径的分类，提出了基于形式化验证的自动化多周期路径检测方式，并通过 Jasper 形式化验证工具进行实验验证，实验证明该方法无需验证人员深入了解设计者意图和电路功能，就能有效可靠地检测出多周期路径，有助于测试人员减少对多周期路径的错误处理，有助于提升验证和设计效率，缩短验证周期。

参考文献：

[1] 郭摇蒙，田摇泽. 数字集成电路多周期路径的设计实现方法[J]. 计算机技术与发展，2013 (8)：204－206.

[2] SYNOPSYS. Synopsys timing constraints and optimization user guide version D-2010.03 [Z]. Synopsys，2010.

[3] Hook's Law. Simple harmonic oscillator [M]. Cambridge，MA，USA：MIT OCW，2021.

[4] BACHMANN E R. Intertial and magnetic tracking of limb segment orientation for inserting humans into synthetic environments [D]. California：Naval Postgraduate School，2000.

[5] ZHANG F B，HO C Y，PENG S L. Static timing analysis and its application in IC design [J]. Chinese Journal of Electron Devices，2006 (29)：1330－1333.

[6] 陈　敏，殷瑞祥，郭　瑢，等. 静态时序分析在数字 ASIC 设计中的应用 [J]. 计算机与自动化，2005 (19)：52－55.

[7] 吴　丹，刘三清，徐维锋. 深亚微米 ASIC 设计中的时序约束与静态时序分析 [J]. 电子工程师，2004，30 (3)：16－19，22.

[8] 虞　蕾，赵宗涛. PSL 逻辑及验证技术研究进展与展望 [J]. 计算机应用研究，2010，27 (7)：2414－2420.

[9] TALUPURU K R，ATHI S. Clock domain crossing glitch detection using formal verification [Z/OL]. MIPS Technologies，2010.

[10] 夏宏美，李成诗. 深亚微米超大规模集成电路的静态时序分析 [J]. 微计算机信息，2006 (8)：215－218.

[11] 王秀芹. 基于 SAT 的数字电路形式验证方法研究 [D]. 哈尔滨：哈尔滨工程大学，2009.

[12] SMITHD R，FRANZON P D. 面向数字系统综合的 Verilog 编码风格 [M]. 汤华莲，田摇泽，译. 西安：西安电子科技大学出版社，2007.

(下转第 97 页)