第 24 卷 第 3 期 电 子 与 信 息 学 报 Vol.24 No.3
2002 年 3 月 JOURNAL OF ELECTRONICS AND INFORMATION TECHNOLOGY Mar. 2002

面向对象方法在可编程逻辑部件分析技术研究中的应用 [1]

蒋雄飞 张 莉 居 悌 *

(深圳证券通信公司 深圳 518040)
*(南京邮电学院计算机科学与技术系 南京 210003)

摘 要 在黑箱辨识方法论的基础上，已经完成了对加密可编程逻辑器件的无损伤破译，所提出的局部穷举法理论，成功解决了在微机环境下大数据量的快速采集和处理问题．该文沿着面向对象方法的新发展趋势，从面向对象分析与设计的角度出发，提出对加密可编程逻辑器件的无损伤破译的一种改进方法．

关键词 面向对象，黑箱分析，可编程逻辑器件
中图号 TP31, TP312

1 引 言

在可编程逻辑器件中，如 PAL 、 GAL 和某些单片机的内含 EPROM 都具有保密功能，这种器件的保密功能主要是在器件的物理结构中设置了保密位。当保密位被编程后，用一般 PLD 开发系统直接访问逻辑阵列的方法就无法读出它们的内容。在已完成的国家自然科学基金资助项目——可编程逻辑部件分析技术的研究中，提出了局部穷举法理论，解决了在微机环境下大数据量的快速采集和处理问题，并成功地应用于加密可编程逻辑器件的无损伤破译。本文结合面向对象方法发展的新思路，从面向对象分析与设计的角度出发，以 GAL 器件的分析为例，利用面向对象方法对分析过程进行改造，以期获得更高的系统处理效率、可靠性、可维护性和可移植性。

2 黑箱辨识方法

黑箱辨识方法是系统科学中的主要方法之一。人们在从事科学研究时，常常会由于种种条件限制，对某些需要认识或控制的系统 (称为客体) 的内部结构和机理不能或不便直接观察到，仿若一个不透明的密封箱子，将这种客体形象地称为黑箱。所谓黑箱辨识方法，就是通过考察黑箱的输入、输出及其动态过程，而不是通过直接考察其内部结构，来定量地研究黑箱的功能特性、行为方式，从而探索其内部结构和机理。它一般包括三个基本步骤，即黑箱的确认、黑箱的考察和建立黑箱模型。黑箱辨识在可编程逻辑部件分析技术中有着很重要的应用。被编程并加密后的 GAL 芯片具有典型的黑箱特征，其本身是研究客体，周围的环境是被应用的电路系统，所以应用黑箱辨识方法分析 GAL 器件是合适和恰当的。

3 面向对象方法

计算机解决问题的方法实质上是从问题域到问题解空间的一种映射，如果这种映射能以人们通常的思维方式来解决，则可以极大地提高软件的开发效率、可靠性和可维护性。面向对象方法学的基本原则是：按人们通常的思维方式建立问题域的模型，尽可能自然地表现求解问题的软件设计方法，即不是以控制为中心，而以事物 (对象) 的行为为中心来考虑计算机上的处理体系。进入 90 年代后，面向对象方法在计算机科学技术领域占领了无可争议的主流地位。现在的面向对象方法突破传统的计算机软件范围，发展到了计算机软件以外的一些领域，如计算机体系结构和人工智能等。面向对象方法在软件工程领域的运用称为面向对象的软件工程方法。它包括面向对象的分析 (OOA) 、面向对象的设计 (OOD) 、面向对象编程 (OOP) 等主要内容。程序员的一个完整的问题解决过程应该本着 OOA→OOD→OOP 的顺序。 OOA 强调直接针对

[1] 2000-05-10 收到， 2001-01-25 定稿
国家自然科学基金（项目编号为 69173318 ）资助

问题域中客观存在的各项事物设立 OOA 模型中的对象，用对象的属性和服务分别描述事物的静态特征和行为。 OOD 是针对系统的一个具体的实现运用面向对象方法，它包括两方面的工作，一是把 OOA 模型直接移植到 OOD ，作为 OOD 的一部分。一是针对具体实现中的人机界面、数据存储、任务管理等因素补充一些与现实有关的部分。这些部分与 OOA 采用相同的表示法和模型结构。 OOA 和 OOD 阶段完成认识问题域与设计系统成分的工作。 OOP 是用一种面向对象的编程语言把 OOD 模型中的每个成分书写出来。《软件工程百科全书》中指出“面向对象开发技术的焦点不应该只对准编程阶段，而应更全面地对准软件工程的其他阶段，面向对象方法真正意义深远的目标是它适合于解决分析与设计期间的复杂性，并实现分析与设计的复用。”基于这一事实，人们对面向对象方法的研究重点，从早期的面向对象编程，转移到面向对象的分析与设计。在本文中将把事物的形象 (数据) 同其意义、功能 (过程) 一体化，建立系统模型，并抽象出处理的基本单位来分析可编程逻辑器件。在首先建立的对象模型中，必须独立出不同的对象，综合功能抽象和数据抽象，完成数据和方法的封装。在各个对象之间采用消息传递机制来激活不同的状态，从而完成对象之间的交互行为。面向对象方法中的这种消息传递机制可以很自然地与并行处理技术、多机系统及网络通信等模型取得一致。有助于系统处理效率的提高，方便系统的移植，实现其高可靠性、高可维护性。

4 系统建模

分析加密 GAL 芯片的主要工作在于前处理机的预处理。预处理主要包括 4 个方面：编程类型判别、组态判别、剔除无关变量和最小项采集。当预处理部分确定的有效最小项送入主机 (后台机) 后，进行以逻辑化简为核心的后台机处理，并最终输出分析结果。逻辑化简主要包含质蕴涵项集合和最小覆盖的求解。详细资料可参见文献 [1] 。

4.1 对象分析与设计

我们提出的面向对象的设计方案从结构上主要分为两个部分：前处理机部分、后台处理机部分。前处理机主要包括 6 个对象类，分别为输入输出类、编程类别 / 组态判别类、时序型编程芯片的预加载类、剔除无关向量类、采集最小项类、数据传送类。后处理机主要包括求质蕴涵项集合类、最小覆盖类。其中编程类别 / 组态判别类为主动对象类 (Active Object Class) 。主动对象类的实例定义为主动对象，这是一个近几年才得以深入讨论和认识的 OO 概念。此前，人们所理解的对象概念实际上只是被动对象，即对象的每个服务都是响应从外部发来的消息才被动执行的。主动对象是至少有一个服务不需要接收消息就能主动执行的对象，引入主动对象可以从系统建模之时就开始用对象表达问题域中的事物的主动行为和系统中的每个任务，使模型与程序以对象为单位的关系更为完善。

在输入输出类中封装了输入变量组合，该类主要根据输入变量组合向硬件施加测试信号并采集结果。编程类别 / 组态判别类中封装的数据结构主要有 LOGIC,IA,IB 。 LOGIC 记录两串状态完全不同的逻辑序列，用以判别芯片的编程类别。 $IA = [I1 \cdots I8E1 \cdots E6]$, $IB = [I(1) \cdots I(8)]$, 其中 $I(j)$ 定义为输出 $F(J)$ 对应的激励， $F(J)$ 对应的输出记为 $O(J)$ 。通过确定芯片受 LOGIC,IA,IB 的控制情况，可以判别出芯片的编程类别及组态。时序型编程芯片的预加载类中封装的主要是激励数据和预加载序列表。剔除无关变量类在其内部封装的数据主要是各输入变量的组合，用以确定与某个输出函数相关的变量。采集最小项类利用其封装的输入激励变量组合完成对某个输出的最小项有序采集。数据传送类则将待传送的数据发往后台处理机。后台机上的求质蕴涵项集合类包含了最小项集合，通过再改进的 Quine-McCluskey (QM) 算法可以求出全部质蕴涵项集合。而最小覆盖类则根据最小项集合及质蕴涵项集合完成对最小覆盖的求解。图 1 为系统对象图的主要部分，图中各个矩形框体单元分别表示所划分的不同类，带有 @ 标记的矩形框体描述的是主动对象类。矩形框体的最上部是类名，中间部分是主要涉及到的数据，最下面记有主要涉及的操作 (过程) 。各单元间的带箭头流线标记出整个系统的消息流动情况。为叙述方便直观起见，在每个类的上方或下方标注出一个其相应的对象名，分别为 INPUT/OUTPUT, PROG-TYPE, PRE-ADD, FIND-RELATION, GET-LEAST, DATA-TRANS, Z-OUT,C-MIN 。

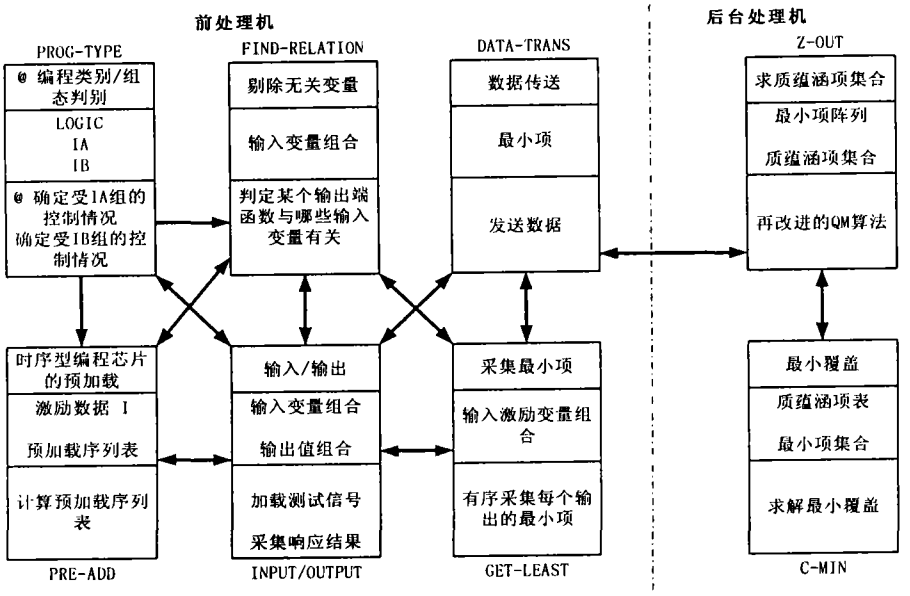

图 1　系统对象及消息流动图

4.2 消息传递

在前处理机部分，对象 PROG-TYPE 利用消息传递机制，将 LOGIC 作为消息传递给 INPUT/OUTPUT 对象。INPUT/OUTPUT 将传来的 LOGIC 作为输入变量组合，向芯片施加测试信号，并采集响应结果。随后利用消息传递将采集到的响应结果返回对象 PROG-TYPE。PROG-TYPE 根据消息返回判别芯片编程类型。当进行组态判别时需要用到输入变量 IA,IB，先确定受 IA 的控制情况，再确定受 IB 的控制情况，完成所有的编程类别和组态判别动作后，即可利用消息激活对象 FIND-RELATION。在 FIND-RELATION 中，根据通过消息传递来的编程类别和组态情况，在内部生成输入变量的组合，并通过激活 INPUT/OUTPUT 后所得到的返回值来确定与某个输出函数相关的变量。为提高系统处理时间，考虑在确定了与某个输出函数相关的所有变量后，就去激活对象 GET-LEAST。由 GET-LEAST 根据收到的消息 (与某个输出函数相关的所有变量) 对该输出的最小项有序采集，当然在采集的过程中依然需要激活 INPUT/OUTPUT 对象。完成对一个输出的最小项有序采集后，激活对象 DATA-TRANS，由 DATA-TRANS 负责将所得结果送入后台处理机。在 DATA-TRANS 传送数据的同时，GET-LEAST 可激活 FIND-RELATION 来确定与下一个输出函数相关的所有变量。这样实际上就实现了 INPU/OUTPUT 与数据向后台处理机传输的并行处理。INPU/OUTPUT 根据接受到的不同输入变量组合，既可对引脚进行串位处理，也可对引脚进行并位处理，还可以多个输入变量组合进行批处理。极大地提高了系统处理的灵活性，节约了系统处理时间。值得一提的是，以上的消息流动分析主要是针对组合型编程芯片进行的。对于时序型编程芯片的分析方法基本相同，不同的主要是需要对输出寄存器进行预加载，以及如何施加时钟脉冲。我们利用对象 PRE-ADD 去完成相应的动作。在 PROG-TYPE 判别出芯片为时序型后，激活 PRE-ADD,PRE-ADD 根据消息生成激励数据和预加载序列表，然后激活对象 FIND-RELATION。

当预处理部分结束且所有输出的有效最小项均被传送到后台机后，即激活对象 Z-OUT，通过再改进的 QM 算法求出全部质蕴涵项集合。随后激活对象 C-MIN，由该对象根据消息传入的全部质蕴涵项集合结合有关最小项完成对最小覆盖的求解。自此，以再改进的 QM 算法和最小覆盖为核心的逻辑化简部分顺利完成，接下来进行一些常规的系统处理即可，如用户界面

设计、输出等。

5 系统改进特点

虽然有一些研究表明，消息传递的开销大约是过程调用开销的 1.75 倍。然而，因为硬件速度已有大幅度的提高，并且消息传递比过程调用可完成更多的工作 (这也正是面向对象技术飞速发展的原因)。所以，考虑利用面向对象的技术来改造系统是可以的。在与原系统的比较中，主要有以下几点是我们作了改进的：

(1) 提出利用面向对象的方法对系统进行重新改造，主要是从软件设计的角度出发，强调了对数据和方法的封装。使得程序结构更加清晰、易读。易于与发展的新技术相结合来进行更深入的研究与应用。

(2) 利用消息传递机制，确保软件可靠性、灵活性。软件之间的依赖性减弱，有益于程序的维护和移植。

(3) 通过代码的重用，可减少总的代码量，并提高程序员的工作效率。

(4) 通过对象的划分，使得对象之间在一定程度上可以并行执行，有效地缩短了系统处理时间。特别是，将施加激励信号并采集结果与数据向后台处理机传送这两部分操作并行起来以后，可以显著的提高整个系统处理速度。

6 结 束 语

利用面向对象方法来改造加密 GAL 器件分析系统，具有一定的创新意义。将面向对象的思想运用于可编程逻辑部件的分析，可以紧密结合当今计算机发展趋向。尤其是从软件开发的角度来说，可以极大地提高编程效率，提高系统的可移植性、可维护和可扩充性，给系统带来的最显著也是最直接的改变将是整个系统处理时间的缩短。并且有助于今后在对可编程逻辑部件分析的基础上，展开进一步应用。

参 考 文 献

[1] 居悌，可编程逻辑器件的开发与应用，北京，人民邮电出版社，1995, 215–227.

[2] 任旭鸣等，集成电路新技术展望，江苏，电子工程师，1999, (9), 1–3.

[3] 邵维忠等，面向对象的系统分析，北京，清华大学出版社，1998, 27–46.

[4] 徐德启等，面向对象基础与 C++ 程序设计教程，兰州，兰州大学出版社，1996, 13–65.

APPLICATION OF OBJECT ORIENTED METHOD IN THE STUDY OF PROGRAMMABLE LOGIC DEVICE ANALYSIS

Jiang Xiongfei Zhang Li Ju Ti*

(*Shenzhen Securities Satellite Communication Co. LTD., Shenzhen* 518040, *China*)

*(*Department of Computer Science and Technology, Nanjing Institute of Posts and Communication, Nanjing* 210003, *China*)

Abstract Based on black box analysis, the unharmed decryption of the encrypted programmable logic device has been realized successfully with Local Exhaustion Approach(LEA) which is proposed to deal with enormous data acquisition and processing in PC. With the development tendency of object oriented method, an improved method for the unharmed decryption of the encrypted programmable logic device is given from object oriented analysis and object oriented design.

Key words Object oriented, Black box analysis, Programmable logic device

蒋雄飞： 男，1975 年生，硕士生，研究方向：数据的快速采集与处理、TMN、证券通信.

张 莉： 女，1976 年生，研究方向：计算机通信、证券通信.

居 悌： 男，1942 年生，教授，研究方向：数据的快速采集与处理、TMN.