

**ĐẠI HỌC THÁI NGUYÊN**  
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**



**NGUYỄN THANH BẰNG**

**PHÂN TÍCH TÍNH CHƯƠNG TRÌNH**  
**BẰNG PHƯƠNG PHÁP GIẢI THÍCH TRỪU TƯỢNG**

**LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH**

**Thái Nguyên, năm 2013**

**ĐẠI HỌC THÁI NGUYÊN**  
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**



**NGUYỄN THANH BẰNG**

**PHÂN TÍCH TÍNH CHƯƠNG TRÌNH**  
**BẰNG PHƯƠNG PHÁP GIẢI THÍCH TRỪU TƯỢNG**

*Chuyên ngành* : KHOA HỌC MÁY TÍNH

*Mã số* : 60.48.01

NGƯỜI HƯỚNG DẪN KHOA HỌC:  
TS. Nguyễn Trường Thắng

**Thái Nguyên, năm 2013**

## **LỜI CAM ĐOAN**

Tôi xin cam đoan tất cả những nội dung được trình bày trong nội dung luận văn đều do tôi nghiên cứu và viết ra dưới sự hướng dẫn của TS. Nguyễn Trường Thắng – Viện Công nghệ thông tin – Viện Khoa học và công nghệ Việt Nam hướng dẫn. Không hề có bất cứ sự sao chép nào ngoài việc tham khảo từ các tài liệu như đã trình bày trong phần tài liệu tham khảo. Nếu có một hình thức gian lận nào tôi xin hoàn toàn chịu trách nhiệm.

Thái Nguyên, tháng 01 năm 2013

Học viên cao học khóa 9.

Chuyên ngành: Khoa học máy tính.

Trường đại học Công nghệ thông tin và truyền thông

Đại học Thái Nguyên

## MỤC LỤC

LỜI CAM ĐOAN.....	2
MỤC LỤC.....	3
DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT.....	5
DANH MỤC CÁC THUẬT NGỮ.....	6
DANH MỤC CÁC HÌNH.....	7
MỞ ĐẦU.....	8
CHƯƠNG I. TỔNG QUAN.....	10
1.1. Công nghệ phần mềm và các vấn đề liên quan.....	10
1.1.1. Khái niệm về công nghệ phần mềm.....	10
1.1.2. Quy trình phát triển phần mềm.....	11
1.2 Các kỹ thuật trong công nghệ phần mềm nhằm nâng cao chất lượng phần mềm.....	13
1.2.1. Kiểm chứng phần mềm.....	14
1.2.2. Phân tích mã nguồn tĩnh.....	15
1.2.3. Kiểm thử phần mềm.....	17
1.2.4. So sánh giữa kiểm chứng mô hình và kiểm thử phần mềm.....	18
1.3 Kết luận chương 1.....	18
CHƯƠNG II. PHƯƠNG PHÁP GIẢI THÍCH TRỪ TƯỢNG.....	19
2.1. Khái niệm giải thích trừu tượng.....	19
2.2. Ứng dụng của giải thích trừu tượng.....	19
2.3. Một số khái niệm cơ bản.....	20
2.3.1. Ngữ nghĩa.....	20
2.3.2. Tính an toàn:.....	20
2.3.3. Giải thích trừu tượng:.....	21
2.3.4. Tiêu chuẩn trừu tượng hóa:.....	22
2.3.5. Miền trừu tượng: ( <i>Abstract domains</i> ):.....	22
2.3.6. Vết thực thi.....	23
2.3.7. Thu thập ngữ nghĩa:.....	25
2.4. Nền tảng toán học của giải thích trừu tượng.....	26
2.4.1. Liên kết nhị phân.....	26

2.4.2. Tập có thứ tự từng phần (Poset).....	26
2.4.3. Cấu trúc dàn (Lattices).....	27
2.4.4. Sơ đồ Hasse.....	28
2.4.5. Điểm cố định (Fixpoint).....	28
2.4.6. Bước lặp.....	29
2.4.7. Kết nối Galois.....	29
2.5. Giải thích trừu tượng.....	29
2.5.1. Đối tượng trừu tượng (Abstract objects).....	30
2.5.2. Thuộc tính trừu tượng.....	31
2.5.3. Giải thích trừu tượng trong phân tích tĩnh chương trình:.....	32
2.5.4. Kết luận chương 2.....	34
<b>CHƯƠNG III. CHƯƠNG TRÌNH THỰC NGHIỆM.....</b>	<b>35</b>
3.1. Giới thiệu về TVLA.....	35
3.2. Nền tảng toán học của TVLA.....	36
3.2.1. Giá trị 3-logic.....	37
3.2.2. Phương pháp.....	39
3.3. Phân tĩnh tĩnh chương trình sử dụng TVLA.....	43
3.3.1. Bài toán 1.....	43
3.3.2. Bài toán 2.....	48
3.4. Kết luận chương 3.....	53
<b>KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN.....</b>	<b>54</b>
<b>TÀI LIỆU THAM KHẢO.....</b>	<b>55</b>
<b>PHỤ LỤC.....</b>	<b>56</b>
1. Thuật toán phân tích mối quan hệ vô hạn thông qua lặp tiến/lùi chi tiết. .....	56
2. Các định nghĩa chức năng trừu tượng trong action.tvp.....	57
3. Các định nghĩa chức năng trừu tượng trong predicates.tvp.....	62
4. Dữ liệu đầu vào của TVLA phân tích chức năng tạo danh sách liên kết creat.tvp.....	64

## DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

STT	Từ viết tắt	Viết đầy đủ	Nghĩa
1	EASL	Engineering Analysis and Simulation Language	Kỹ thuật Phân tích và ngôn ngữ mô phỏng
2	CM	Summary nodes	Nút đại diện
3	PTTGTT	Phân tích tĩnh chương trình bằng giải thích trừu tượng.	
4	CFG	Control Flow Graphc	Sơ đồ luồng điều khiển.

## DANH MỤC CÁC THUẬT NGỮ

STT	Thuật ngữ	Ý nghĩa
1	Vết thực thi (Trace semantics)	Tập hợp các dấu vết về quá trình chuyển đổi trạng thái của chương trình.
2	Tập có thứ tự từng phần (Poset - Partial Ordered Set)	Là một tập hợp các phần tử có thứ tự
3	Cấu trúc dàn (Lattice)	Là một tập hợp các phần tử có thứ tự từng phần có điểm chặn dưới lớn nhất và trên nhỏ nhất

## DANH MỤC CÁC HÌNH

STT	Hình sử dụng
1	Hình 1.1: Mô hình tổng quát quy trình sản xuất phần mềm trong xe hơi
2	Hình 1.2: Tổng quan phân tích mã nguồn tĩnh
3	Hình 1.3: MISRA-C là “Subset”-Tập con của ngôn ngữ C
4	Hình 1.4: Hai cuốn MISRA-C:1998 và MISRA-C:2004
5	Hình 2.1 Sơ đồ hành vi của chương trình
6	Hình 2.2 Quỹ đạo an toàn
7	Hình 2.3 Quỹ đạo không an toàn
8	Hình 2.4 Quỹ đạo hành vi trừu tượng của chương trình.
9	Hình 2.4 Phát hiện lỗi với giải thích trừu tượng
10	Hình 2.5 Các bước chuyển trạng thái của chương trình
11	Hình 2.6 Vết thực thi của chương trình
12	Hình 2.7 Thu thập ngữ nghĩa của chương trình
13	Hình 2.8 Đồ thị liên kết nhị phân
14	Hình 2.9 Thuật toán giải thích trừu tượng tổng quát
15	Hình 3.1 Bảng giá trị phép giao 3-logic
16	Hình 3.2 Bảng giá trị phép hợp 3-logic
17	Hình 3.3 Bảng giá trị phép hợp 3-logic.
18	Hình 3.4 Bảng trừu tượng hóa bằng logic vị từ
19	Hình 3.5 Mô phỏng trạng thái bộ nhớ cấu trúc con trỏ.
20	Hình 3.6 Trạng thái chương trình sử dụng 2-logic
21	Hình 3.7 Trạng thái chương trình sử dụng nút đại diện (3-logic)
22	Hình 3.8 Tiến trình làm việc của một quá trình PTTGTTT
23	Hình 3.9 Thực hiện phân tích tĩnh chương trình bằng TVLA.
24	Hình 3.10. Kết quả phân tích chức năng tạo danh sách liên kết
25	Hình 3.11. Trạng thái tổng thể chương trình thêm một nút vào cây nhị phân



## MỞ ĐẦU

Ngày nay, phần mềm xuất hiện ở khắp mọi nơi và trong hầu hết các thiết bị điện tử đều sử dụng phần mềm trong đó. Phần mềm không đơn giản là chương trình trên máy tính mà nó bao gồm cả tư liệu lưu trữ và thông tin vận hành giúp chương trình có thể hoạt động được. Vì những ứng dụng to lớn của phần mềm trong các ngành sản xuất, tài chính ngân hàng, y tế, bệnh viện, trường học, nhà nước,...nên yêu cầu rất lớn đặt ra đó là xây dựng, phát triển và ứng dụng công nghệ phần mềm.

Trong luận văn này tôi xin giới thiệu một phương pháp kiểm tra đánh giá chất lượng phần mềm mới đó là phân tích tĩnh chương trình. Với mục tiêu: Đưa ra một cách nhìn nhận mới về việc lập xây dựng và kiểm tra sự đúng đắn của chương trình đó là sử dụng phương pháp phân tích tĩnh chương trình. Áp dụng các công cụ để phân tích chương trình, kiểm tra sự đúng đắn của chương trình bằng giải thích trừu tượng (Abstract Interpretation). Vì đây là một kỹ thuật phân tích chương trình chưa được nghiên cứu rộng rãi ở Việt Nam, nên luận văn này mang tính giới thiệu ban đầu về khái niệm cơ bản và nền tảng lý thuyết dựa trên tài liệu gốc [2], là giáo trình được sử dụng trong đào tạo thạc sỹ của Học viện Công nghệ Massachusetts (MIT) – Hoa Kỳ, trong chương 2. Phần thử nghiệm trong chương 3 tập trung vào việc cài đặt và thử nghiệm bộ công cụ TVLA (3-Valued Logic Analysis Engine) của trường đại học Khoa Học Máy Tính Tel Aviv (School of Computer Science Tel Aviv University), thành phố Tel Aviv, Isarel[6]. Công cụ này phân tích chương trình sử dụng giải thích trừu tượng.

Nội dung luận văn gồm 3 chương:

### CHƯƠNG I. TỔNG QUAN

Đưa ra các khái niệm liên quan, sự cần thiết của việc phân tích tĩnh chương trình, giới thiệu các phương pháp phân tích tĩnh chương trình.

### CHƯƠNG II. PHƯƠNG PHÁP GIẢI THÍCH TRỪU TƯỢNG

Trình bày nền tảng lý thuyết, thuật toán, ứng dụng, ưu nhược điểm của phương pháp giải thích trừu tượng.[2]

### CHƯƠNG III. CHƯƠNG TRÌNH THỰC NGHIỆM

Cài đặt phương pháp phân tích tĩnh bằng giải thích trừu tượng, đưa ra kết quả thực nghiệm và kết luận[6]