

## THÔNG TIN VỀ LUẬN ÁN TIẾN SĨ

1. Họ và tên nghiên cứu sinh: Lê Chí Luận
2. Giới tính: Nam
3. Ngày sinh: 08/03/1980
4. Nơi sinh: Thanh Hóa
5. Quyết định công nhận nghiên cứu sinh số: 827/QĐ - ĐT ngày 03 tháng 11 năm 2011 của Giám đốc Đại học Quốc gia Hà Nội công nhận là nghiên cứu sinh đào tạo tại Trường Đại học Công nghệ.
6. Các thay đổi trong quá trình đào tạo: Quyết định số 47/QĐ-ĐT ngày 25 tháng 01 năm 2013 về việc bổ sung cán bộ hướng dẫn nghiên cứu sinh của Hiệu trưởng Trường Đại học Công nghệ. Tập thể cán bộ hướng dẫn mới cho nghiên cứu sinh Lê Chí Luận như sau:  
Cán bộ hướng dẫn chính: TS. Phạm Ngọc Hùng, Trường ĐH Công nghệ  
Cán bộ hướng dẫn phụ: PGS. TS. Hồ Sĩ Đàm, Trường ĐH Công nghệ
7. Tên đề tài luận án:  
***Đặc tả và kiểm chứng từng phần cho phần mềm dựa trên biểu đồ tuần tự***
8. Chuyên ngành: Kỹ thuật Phần mềm
9. Mã số: 62.48.01.03
10. Cán bộ hướng dẫn khoa học:  
1. PGS. TS. Phạm Ngọc Hùng  
2. PGS. TS. Hồ Sĩ Đàm

### 11. Tóm tắt các kết quả mới của luận án:

Luận án đã đạt được các kết quả chính sau:

Đề xuất một phương pháp hoàn chỉnh nhằm tự động sinh mô hình và kiểm chứng từng phần cho các thiết kế phần mềm được đặc tả bằng biểu đồ tuần tự UML 2.0. Ý tưởng chính của phương pháp này là tự động sinh mô hình đặc tả chính xác hành vi của các biểu đồ tuần tự biểu diễn dưới dạng các máy hữu hạn trạng thái được gán nhãn (LTSs). Các mô hình này cùng với thuộc tính được kiểm chứng (chỉ cho các thuộc tính an toàn) sẽ được cung cấp cho phương pháp kiểm chứng giả định – đảm bảo nhằm kiểm chứng tính đúng đắn của hệ thống mà không cần ghép nối các mô hình của các thành phần lại với nhau. Bằng cách áp dụng phương pháp kiểm chứng này, bài toán bùng nổ không gian trạng thái hứa hẹn được giải quyết. Một công cụ hỗ trợ cũng đã được cài đặt và thực nghiệm với một số ví dụ điển hình nhằm minh chứng cho tính đúng đắn và tính hiệu quả của phương pháp đề xuất.

Đề xuất một phương pháp sinh mô hình được biểu diễn dưới dạng các ô tô măt vào/ra cho các đối tượng từ biểu đồ tuần tự UML 2.0. Với phương pháp đặc tả này, chúng ta không làm mất tính hướng đối tượng của thiết kế phần mềm trong các biểu đồ tuần tự. Nghiên cứu này cũng đề xuất một phương pháp chuyển đổi từ đặc tả dưới dạng ô tô măt vào/ra sang đặc tả PROMELA để có thể sử dụng bộ công cụ SPIN nhằm kiểm chứng tính đúng đắn của hệ thống. Với giải pháp này, chúng ta có thể kiểm chứng nhiều loại thuộc tính hơn so với việc chỉ hỗ trợ thuộc tính an toàn như đóng góp đầu tiên của luận án. Một công cụ hỗ trợ phương pháp đề xuất cũng đã được cài đặt và thực nghiệm với một số hệ thống đơn giản và thu được kết quả khả quan bước đầu.

Đề xuất hai cải tiến nhằm nâng cao tính hiệu quả của phương pháp kiểm chứng giả định – đảm bảo sử dụng thuật toán học  $L^*$  - được biết đến như là một phương pháp tiềm năng nhằm giải quyết bài toán bùng nổ không gian trạng thái trong kiểm chứng mô hình. Cải tiến thứ nhất tập trung vào việc giảm thiểu các truy vấn lặp lại và giải pháp lựa chọn hậu tố (suffix) khi xử lý các phần ví dụ trong quá trình học và sinh các ứng cử viên giả định của thuật toán  $L^*$ . Với cải tiến này, tính hiệu quả của phương pháp kiểm chứng giả định – đảm bảo được cải thiện đáng kể. Một công cụ hỗ trợ cũng đã được cài đặt và áp dụng cho một số ví dụ điển hình nhằm minh chứng cho tính hiệu quả của những cải tiến này. Cải tiến thứ hai là đề xuất một giải pháp mới nhằm sinh ra các giả định có ngôn ngữ nhỏ nhất (giả định nhỏ nhất) so với các giả định được sinh ra bởi phương pháp hiện tại. Các giả định này sẽ hiệu quả hơn trong việc kiểm chứng lại tính đúng đắn của hệ thống trong tương lai khi một số thành phần bị thay đổi.

## **12. Khả năng ứng dụng trong thực tiễn:**

Các kết quả của luận án có thể công cụ hóa nhằm kiểm chứng tính đúng đắn của các thiết kế phần mềm.

## **13. Những hướng nghiên cứu tiếp theo:**

Trong nghiên cứu thứ nhất, tác giả đang nghiên cứu để áp dụng phương pháp này với một số hệ thống thực tế và lớn hơn để chứng minh tính hiệu quả của nó. Kiểm chứng được các thuộc tính không chỉ là thuộc tính an toàn (liveness, fairness). Đồng thời, tác giả đang mở rộng phương pháp sử dụng các dạng biểu đồ UML khác của giai đoạn thiết kế (ví dụ như: sơ đồ lớp, sơ đồ các trạng thái v.v.) để các hệ thống nhất định có thể xác nhận trong tất cả các khía cạnh của thiết kế tự động. Tác giả sẽ tiến hành chứng minh về mặt lý thuyết tính đúng đắn của phương pháp sinh mô hình và kiểm chứng tính đúng đắn thiết kế cho các phần mềm dựa trên thành phần.

Trong nghiên cứu thứ hai, đề xuất phương pháp kiểm chứng từng phần cho đặc tả ô tô măt vào/ra. Đề xuất phương pháp kiểm chứng từng phần cho đặc tả ô tô măt vào/ra và mở rộng các ô tô măt có yếu tố thời gian. Phương pháp này còn có thể kết hợp với các giải pháp kiểm chứng từng phần nhằm giải quyết bài toán bùng nổ không gian trạng thái

trong kiểm chứng mô hình. Về mặt thực nghiệm, nghiên cứu sẽ thử nghiệm công cụ đã được xây dựng với các thiết kế trong thực tế. Một giao diện đồ họa cũng sẽ được xây dựng nhằm giúp công cụ trở nên trực quan, dễ sử dụng, có thể áp dụng vào quy trình phát triển phần mềm tại các công ty.

Trong nghiên cứu thứ ba, chúng tôi đang tiến hành các thực nghiệm để minh chứng cho tính hiệu quả của các giả định nhỏ nhất được sinh ra bởi đề xuất này. Tác giả đang trong quá trình hoàn thiện để tìm ra giả định có ngôn ngữ nhỏ nhất. Bên cạnh đó, nghiên cứu đang trong quá trình áp dụng các phương pháp đề xuất cho phần mềm trong thực tế để chứng minh hiệu quả của phương pháp. Thêm nữa, tác giả đang nghiên cứu làm thế nào để khái quát phương pháp cho các hệ thống lớn hơn, như hệ thống chứa nhiều hơn hai thành phần. Hơn nữa, công việc hiện tại là chỉ áp dụng cho các thuộc tính an toàn, tác giả sẽ mở rộng phương pháp đề xuất của để kiểm tra các thuộc tính khác như thuộc tính liveness, thuộc tính fairness. Từ đó áp dụng các phương pháp đề xuất cho các hệ thống nói chung như các hệ thống phân cứng, hệ thống thời gian thực. Nghiên cứu thứ ba khi kết hợp với nghiên cứu thứ nhất hướng đến một giải pháp đầy đủ cho việc kiểm chứng tính đúng đắn của các thiết kế có khả năng ứng dụng trong thực tế. Kết hợp các kết quả nghiên cứu của luận án với các phương pháp kiểm chứng phần mềm trong ngữ cảnh tiến hóa để có các giải pháp hiệu quả hơn cũng sẽ được quan tâm nghiên cứu.

#### **14. Các công trình đã công bố có liên quan đến luận án:**

1. Hoang-Viet Tran, Chi-Luan Le, Quang-Trung Nguyen and Pham Ngoc Hung (2014), “An Efficient Method for Automated Generating Models of Component-based Software”, *In Proc. of the 6th International Conf. on Knowledge and Systems Engineering, Springer LNCS*, pp. 499-511.
2. Lê Chí Luân, Phạm Ngọc Hùng (2016), “Phương pháp sinh mô hình tự động cho các biểu đồ tuần tự UML 2.0”, *Kỷ yếu Hội nghị Khoa học Quốc gia lần thứ 9: Nghiên cứu cơ bản và ứng dụng công nghệ thông tin (FAIR 2016)*, pp. 619-625.
3. Hoang-Viet Tran, Chi-Luan Le and Ngoc Hung Pham (2016), “A Strongest Assumption Generation Method for Component-Based Software Verification”, *In Addendum Proc. of the 2016 IEEE-RIVF International Conference on Computing and Communication Technologies*, pp. 1-6.
4. Chi-Luan Le, Hoang-Viet Tran, Pham Ngoc Hung (2016), “A Framework for Modeling and Modular Verifying of Component-based System Designs”, *VNU Journal of Science: Computer Science and Communication Engineering*, vol. 32 , no. 2, pp. 31-42.
5. Chi-Luan Le, Hoang-Viet Tran, and Pham Ngoc Hung (2017). "On Implementation of the Assumption Generation Method for Component-Based

Software Verification." Advanced Topics in Intelligent Information and Database Systems. Springer International Publishing, pp. 549-558.

*Ngày tháng năm 2017*  
**Xác nhận của cán bộ hướng dẫn**  
*(Kí và ghi rõ họ tên)*

*Ngày tháng năm 2017*  
**Nghiên cứu sinh**  
*(Kí và ghi rõ họ tên)*

**INFORMATION ON DOCTORAL THESIS**

1. Full name : Le Chi Luan                          2. Sex: Male  
3. Date of birth: 08/03/1980 ..... 4. Place of birth: Thanh Hoa  
5. Admission decision number: 827/QĐ - ĐT Dated: 03/ 11/2011  
6. Changes in academic process:

Decision number 47/QĐ-ĐT on 25/01/2013 about changing supervisors as follows:

First Supervisor: Assoc. Prof. Pham Ngoc Hung

Second Supervisor: Assoc. Prof. Ho Si Dam

7. Official thesis title:

***Specification and Modular Verification of Software via Sequence Diagrams***

8. Major: Software Engineering ..... 9. Code: 62.48.01.03 .....  
10. Supervisors: Assoc. Prof. Pham Ngoc Hung and Assoc. Prof. Ho Si Dam  
11. Summary of the **new findings** of the thesis:

Proposing a completed method for automated generating models and modular model checking of system's designs represented by UML 2.0 sequence diagrams. The key idea of this method is to generating models that exactly describe behaviors of the given UML 2.0 sequence diagrams. These models are represented by labeled transition systems. The generated models and the required safety properties are given to the assume-guarantee verification method in order to modular model checking of the systems without composing the components together. The proposed method is promising to solve the state space explosion problem. An support tool has been implemented and applied for several typical systems in order to show the correctness and effectiveness of the proposed method.

Proposing a method for generating models that describe behaviors of the objects in the given UML 2.0 sequence diagrams. These models are represented by I/O automata. Instead of generating a model that describes behaviors of the whole sequence diagram, this method generates each model for each object. By this method, the "object-oriented" property of the UML design is conserved. This research also proposes a mechanism for conversing the models represented by I/O automata to PROMELA specifications in order to apply the model checker named SPIN for checking of the systems. The method can

support to check several types of properties (i.e., safety, liveness, fairness, ...) in comparison with the first contribution where the method only supports the safety properties. A tool that supports the proposed method has been developed and tested with some simple case studies. The obtained experimental results are promising.

Proposing two improvements in order to reduce the complexity of the assume-guarantee verification method. This method has been known as a promising solution to deal with the state space explosion problem in model checking of component-based software. The first improvement is a counterexample analysis method that is simple to implement but effective enough to prevent the verification process from infinite loops when considering the last action of counterexample as suffix in implementation. This is done by finding a suffix that can make the observation table not closed when being added to the suffix set of the table and use that suffix for the learning process. Moreover, this improvement also proposes a reduction of the number of membership queries to be asked to teacher when learning assumptions. This results in a significantly faster speed in generating assumption than that of the original algorithm. An implemented tool and experimental results are also described to show the effectiveness of the improvements. The second one presents a method for generating strongest assumptions during component-based software verification. These assumptions will effectively reduce the computational cost when verifying component-based software, especially for large-scale and evolving ones.

12. Practical applicability, if any:

13. Further research directions, if any: .....

14. Thesis-related publications:

1. Hoang-Viet Tran, Chi-Luan Le, Quang-Trung Nguyen and Pham Ngoc Hung (2014), "An Efficient Method for Automated Generating Models of Component-based Software", *In Proc. of the 6th International Conf. on Knowledge and Systems Engineering, Springer LNCS*, pp. 499-511.
2. Lê Chí Luân, Phạm Ngọc Hùng (2016), "Phương pháp sinh mô hình tự động cho các biểu đồ tuần tự UML 2.0", *Kỷ yếu Hội nghị Khoa học Quốc gia lần thứ 9: Nghiên cứu cơ bản và ứng dụng công nghệ thông tin (FAIR 2016)*, pp. 619-625.
3. Hoang-Viet Tran, Chi-Luan Le and Ngoc Hung Pham (2016), "A Strongest Assumption Generation Method for Component-Based Software Verification", *In Addendum Proc. of the 2016 IEEE-RIVF International Conference on Computing and Communication Technologies*, pp. 1-6.
4. Chi-Luan Le, Hoang-Viet Tran, Pham Ngoc Hung (2016), "A Framework for Modeling and Modular Verifying of Component-based System Designs", *VNU Journal of Science: Computer Science and Communication Engineering*, vol. 32 , no. 2, pp. 31-42.
5. Chi-Luan Le, Hoang-Viet Tran, and Pham Ngoc Hung (2017). "On Implementation of the Assumption Generation Method for Component-Based

Software Verification." Advanced Topics in Intelligent Information and Database Systems. Springer International Publishing, pp. 549-558.

Date: .....  
Signature: .....  
Full name: .....

Date: .....  
Signature: .....  
Full name: .....