

**ĐẠI HỌC QUỐC GIA HÀ NỘI**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**

**Trương Xuân Hiếu**

**KỸ THUẬT THỰC THI TƯỢNG TRƯNG**

**VÀ ỨNG DỤNG TRONG KIỂM CHỨNG**

**CHƯƠNG TRÌNH ĐA LUỒNG**

**Khóa luận tốt nghiệp đại học hệ chính quy**

Ngành Công nghệ thông tin

Giảng viên hướng dẫn: Tô Văn Khánh

**Hà Nội - 2023**

**LỜI CẢM ƠN**

Lời đầu tiên, em xin tỏ lòng biết ơn chân thành và sâu sắc tới TS.Tô Văn Khánh – giảng viên làm việc tại trường Đại học Công Nghệ - Đại học Quốc Gia Hà Nội, người đã hướng dẫn tận tình, động viên và giúp đỡ em trong suốt quá trình thực hiện khóa luận tốt nghiệp này.

Em cũng xin gửi cảm ơn tới các quý thầy cô Khoa Công nghệ thông tin nói riêng và trường Đại học Công nghệ - Đại học Quốc gia Hà Nội nói chung, đã dìu dắt, bảo ban em trong thời gian em vẫn còn ngồi ghế nhà trường. Những kiến thức mà các quý thầy cô tận tình truyền đạt đã giúp em có được nền tảng vững chắc trên con đường học tập và làm việc.

Cuối cùng, em xin cảm ơn những tới các anh chị và các bạn, đặc biết là tập thể lớp K64-CD đã đồng hành cùng em trong suốt những năm học qua. Mọi người không chỉ tận tình chia sẻ, giúp đỡ và đưa ra những góp ý chân thành mà còn là chỗ dựa tinh thần, san sẻ niềm vui nỗi buồn, giúp em vượt qua những khó khăn trong học tập cũng như là cuộc sống.

**Mục lục**

[**Lời cam đoan** 5](#_Toc131016004)

[**Tóm tắt** 6](#_Toc131016005)

[**Danh sách kí hiệu** 7](#_Toc131016006)

[**Danh sách bảng biểu** 8](#_Toc131016007)

[**Danh sách hình vẽ** 9](#_Toc131016008)

[**Chương 1. Kiểm chứng chương trình đa luồng** 10](#_Toc131016009)

[**1.1.** **Kiểm chứng** 10](#_Toc131016010)

[**1.1.1.** **Kiểm chứng chương trình** 10](#_Toc131016011)

[**1.1.2.** **Kiểm chứng mô hình** 11](#_Toc131016012)

[**1.2.** **Thực thi đa luồng** 11](#_Toc131016013)

[**1.3.** **Giải pháp kiểm chứng thực thi đa luồng** 12](#_Toc131016014)

[**Chương 2. Kiểm chứng dựa trên kỹ thuật thực thi tượng trưng** 13](#_Toc131016015)

[**2.1.** **Kỹ thuật thực thi tượng trưng** 13](#_Toc131016016)

[**2.1.1.** **Khái niệm** 13](#_Toc131016017)

[**2.1.2.** **Kiến trúc thực thi tượng trưng trong kiểm chứng chương trình đa luồng** 14](#_Toc131016018)

[**2.1.3.** **Trừu tượng hóa trong thực thi tượng trưng** 15](#_Toc131016019)

[**2.2.** **Satisfiability Modulo Theories** 17](#_Toc131016020)

[**Chương 3. Xây dựng phương pháp kiểm chứng chương trình đa luồng ACIO** 18](#_Toc131016021)

[**3.1. Kiểm chứng dựa trên đồ thị thứ tự sự kiện EOG** 18](#_Toc131016022)

[**3.1.1.** **Multi-threaded Program** 18](#_Toc131016023)

[**3.1.2.** **Bounded Model Checking** 20](#_Toc131016024)

[**3.1.3.** **Đồ thị thứ tự sự kiện** 20](#_Toc131016025)

[**3.2. Phương pháp biểu diễn ràng buộc** 22](#_Toc131016026)

[**3.2.1.** **Ràng buộc dựa trên phép gán giá trị** 22](#_Toc131016027)

[**3.2.2.** **Ràng buộc dựa trên liên kết đọc-ghi** 22](#_Toc131016028)

[**3.2.3.** **Ràng buộc suy diễn trên liên kết đọc-ghi** 22](#_Toc131016029)

[**3.3.** **Minh họa phương pháp** 23](#_Toc131016030)

[**3.4.** **Đánh giá với phương pháp đã có** 24](#_Toc131016031)

[**Chương 4. Thực nghiệm đánh giá** 25](#_Toc131016032)

[**Kết luận** 26](#_Toc131016033)

[**Tài liệu tham khảo** 27](#_Toc131016034)

# **Lời cam đoan**

Tôi xin cam đoan rằng những nghiên cứu về phương pháp kiếm chứng chương trình đa luồng được trình bày trong khóa luận này là của tôi và chưa từng được nộp như một báo cáo khóa luận tại trường Đại học Công Nghệ - Đại học quốc gia Hà Nội hoặc bất kỳ trường đại học khác. Những gì tôi viết ra không sao chép từ các tài liệu, không sử dụng các kết quả của người khác mà không trích dẫn cụ thể. Tôi xin cam đoan cốt lõi của công cụ tôi trình bày trong khoá luận là do tôi tự phát triển, không sao chép mã nguồn của người khác.

Nếu sai tôi hoàn toàn chịu trách nhiệm theo quy định của trường Đại Học Công Nghệ - Đại Học Quốc Gia Hà Nội.

Hà Nội, ngày....... tháng....... năm.............

Sinh viên

Trương Xuân Hiếu

# **Tóm tắt**

Sự phát triển bùng nổ của ngành công nghiệp phần mềm trong những năm gần đây đã kéo theo rất nhiều hệ quả. Các phần mềm càng ngày càng lớn dần, càng trở nên phức tạp, việc thực thi các phần mềm đó cũng càng ngày càng tiêu tốn nhiều thời gian.

Để giảm thiểu chi phí về thời gian, khái niệm thực thi đa luồng (multi threading) đã xuất hiện. Thực thi đa luồng giúp phần mềm có thể thực hiện nhiều tác vụ cùng một lúc, giúp giảm thiểu chi phí thời gian đi rất nhiều.

Tuy nhiên, bên cạnh đó, thực thi đa luồng lại vô cùng phức tạp trong trình tự thực thi vì các câu lệnh của chương trình chạy đan xen (interleave) vào nhau, không có một thứ tự cố định, kéo theo đó là sự gia tăng của chi phí kiểm thử. Ngoài ra, các phương pháp kiểm thử truyền thống không thể đảm bảo rằng toàn bộ các trình tự thực thi đều được kiểm thử, dẫn đến việc kiểm thử thiếu, làm kết quả kiểm thử bị sai lệch so với thực tế.

Do đó, nghiên cứu này đề xuất một phương pháp kiểm chứng chương trình đa luồng có tên là All-Conflicts-In-One (ACIO) để thay cho các phương pháp kiểm thử. Phương pháp kiểm chứng này được xây dựng dựa trên phương pháp kiểm chứng Yogar-CBMC.

Phương pháp kiểm chứng Yogar-CBMC sử dụng đồ thị để biểu diễn các hành động đọc/ghi giá trị (Event Order Graph - EOG) của chương trình đa luồng và tìm ra điểm xung đột đọc – ghi giữa các biến dùng chung của các luồng, từ đó xây dựng nên các ràng buộc. Tuy nhiên, với mỗi vòng lặp thực thi, phương pháp Yogar-CBMC chỉ có thể tìm được nhiều nhất một điểm xung đột, do đó đối với các chương trình đa luồng có nhiều điểm xung đột và các điểm xung đột là phức tạp, số vòng lặp thực thi lớn sẽ làm giảm độ hiệu quả và tin cậy của phương pháp này.

Phương pháp kiểm chứng ACIO cũng sử dụng đồ thi EOG làm cơ sở để xác minh các xung đột. Tuy nhiên thay vì tìm kiếm lần lượt các điểm xung đột, phương pháp ACIO sẽ xây dựng nên tập hợp các ràng buộc cho tất cả các hành động đọc – ghi và tìm ra toàn bộ các điểm xung đột chỉ trong một vòng lặp thực thi duy nhất. Chi tiết về phương pháp kiểm chứng ACIO sẽ được trình bày chi tiết trong tài liệu này.

# **Danh sách kí hiệu**

* **ACIO** All-Conflicts-In-One
* **AST** Abstract Syntax Tree
* **BMC** Bounded Model Checking
* **CFG** Control Flow Graph
* **DSE** Dynamic Symbolic Execution
* **EOG** Event Order Graph
* **SMT** Satifiability Modulo Theories
* **SSE** Static Symbolic Execution
* **SV-COMP** Software Verification Competition

# **Danh sách bảng biểu**

# **Danh sách hình vẽ**

# **Chương 1. Kiểm chứng chương trình đa luồng**

* 1. **Kiểm chứng**

*Sự phát triển của công nghệ phần cứng kéo theo sự bùng nổ của ngành công nghiệp phần mềm khiến cho nhu cầu đảm bảo chất lượng phần mềm càng ngày càng được chú ý, đặc biệt là những phần mềm phức tạp, sử dụng kiến trúc đa luồng.*

*Phần lớn các quy trình đảm bảo chất lượng phần mềm hiện nay được xây dựng dựa trên phương pháp kiểm thử. Có thể nói kiểm thử là một phương pháp khá hiệu quả trong việc kiểm tra tính đúng đắn của phần mềm với các đầu vào cụ thể và phổ biến. Tuy nhiên, các đầu vào cụ thể và phổ biến chỉ chiếm một phần rất nhỏ trong toàn bộ các đầu vào khả thi, và dù rằng xác xuất xảy ra của chúng là “phổ biến” không có nghĩa là chúng luôn luôn xảy ra. Điều đó có thể dẫn đến việc bỏ sót nhiều lỗi của chương trình khi thực hiện kiểm thử.*

*Chính bởi sự khiếm khuyết của phương pháp kiểm thử, phương pháp kiểm chứng đã được ra đời nhằm mục tiêu kiểm tra toàn bộ các đầu vào khả thi của chương trình để đảm bảo chương trình hoàn toàn không có lỗi.*

* + 1. **Kiểm chứng chương trình**

Kiểm chứng chương trình (software verification) là quá trình xác minh xem chương trình hoạt động đúng như mong đợi hay không. Trong quá trình kiểm chứng, các kỹ sư phần mềm sẽ sử dụng các kỹ thuật khác nhau để tìm ra các lỗi hoặc sai sót trong chương trình, từ đó cải thiện chất lượng và độ tin cậy của chương trình.

Kiểm chứng chương trình có thể bao gồm các phương pháp kiểm thử (testing) để đảm bảo chương trình hoạt động đúng trong các trường hợp sử dụng thực tế, kiểm tra mã nguồn (code review) để tìm lỗi cú pháp hoặc thiếu sót trong logic của chương trình, hay sử dụng các công cụ phân tích tĩnh (static analysis) để phát hiện các lỗi tiềm ẩn trong mã nguồn.

Mục tiêu của kiểm chứng chương trình là đảm bảo rằng chương trình đáp ứng được yêu cầu và hoạt động đúng, đáng tin cậy và an toàn. Nó là một phần quan trọng trong quá trình phát triển phần mềm và đảm bảo rằng chương trình sẽ không gây ra sự cố hoặc tổn thất.

* + 1. **Kiểm chứng mô hình**

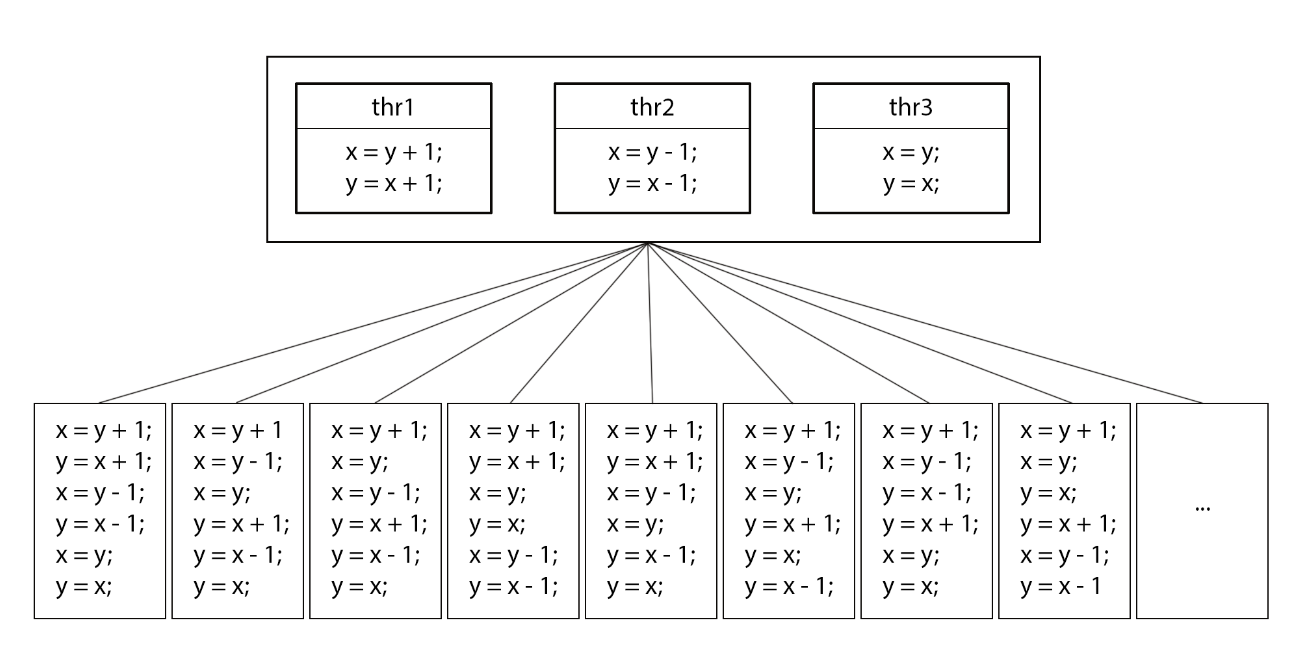
Trong thực tế thiết kế và phát triển phần mềm, công việc kiểm chứng tiêu tốn nhiều thời gian và công sức hơn là việc xây dựng hệ thống. Do đó, nhu cầu tìm kiếm một kỹ thuật kiểm chứng hiệu quả và giảm thiểu tối đa chi phí đang ngày càng trở nên cấp thiết. Các phương pháp hình thức cung cấp một triển vọng tích hợp kiểm chứng với thiết kế hệ thống, qua đó gia tăng độ hiệu quả và giảm thiểu chi phí của việc kiểm chứng.

Kỹ thuật kiểm chứng mô hình là quá trình sử dụng các phương pháp, công cụ và kỹ thuật để đánh giá tính đúng đắn, hiệu quả và đáng tin cậy của mô hình. Kỹ thuật này dựa trên cơ sở mô tả các hành vi của hệ thống thông qua các công thức toán học rõ ràng và chính xác. Về tổng quan, phương pháp kiểm chứng mô hình sẽ kiểm tra tất cả các kịch bản khả thi bằng cách vét cạn toàn bộ các trạng thái của hệ thống. Nhờ đó, kiểm chứng mô hình hoàn toàn có thể khẳng định rằng hệ thống có thật sự thỏa mãn các thuộc tính nhất định nào đó.

Áp dụng lý thuyết về kiểm chứng mô hình, các công cụ kiểm chứng mô hình sẽ kiểm tra tất cả các trạng thái có liên quan của hệ thống. Trong trường hợp một tập các trạng thái nào đó vi phạm đặc tính mà đặc tả mong muốn, một phản ví dụ (counter example) cho thấy cách mà hệ thống hoạt động để tạo ra lỗi sẽ được sinh ra. Nhờ đó, người thiết kế và cài đặt có thể dễ dàng hơn trong việc kiểm tra và gỡ lỗi, đồng thời tích hợp các mô hình phù hợp.

* 1. **Thực thi đa luồng**

Trong kiểm chứng chương trình, thực thi đa luồng là một trong những vấn đề thách thức nhất. Mặc dù trên lý thuyết, các luồng trong chương trình sẽ được thực thi một cách “song song”, tuy nhiên trong thực tế, các câu lệnh trong các luồng không được thực hiện song song mà sẽ đan xen theo rất nhiều cách khác nhau, tạo nên rất nhiều trình tự thực thi vô cùng phức tạp. Do đó, kiểm chứng bằng việc xây dựng các trình tự thực thi dựa trên cách xen kẽ các câu lệnh là không hề đơn giản, chưa kể đến độ phức tạp của chính bản thân các câu lệnh đó.

Hình 1.2.1. Một số trình tự thực thi của chương trình chạy song song ba luồng

* 1. **Kiểm chứng thực thi đa luồng**

Một chương trình, dù đơn giản hay phức tạp, đa luồng hay đơn luồng thì theo góc nhìn của máy tính, chương trình đó cũng chỉ đơn thuần đọc giá trị từ các ô nhớ, thao tác với giá trị đọc được rồi ghi lại vào một số ô nhớ nào đó. Do đó, mã hóa các tín hiệu đọc / ghi giá trị để kiểm tra xung đột thay vì sắp xếp xen kẽ các câu lệnh là một giải pháp vô cùng hữu hiệu trong kiểm chứng chương trình đa luồng. Ngoài ra, việc mã hóa các tín hiệu đọc / ghi giá trị không chỉ rõ ràng mà việc kiểm tra xung đột giữa các tín hiệu còn đơn giản hơn rất nhiều do tập phần tử của chúng chỉ bao gồm hai phần tử đọc và ghi.

Cũng bởi sự phức tạp của chương trình đa luồng và độ hiệu quả của việc mã hóa các tín hiệu đọc / ghi trong việc kiểm tra xung đột, đã có rất nhiều những nghiên cứu về kiểm chứng chương trình đa luồng áp dụng tín hiệu đọc / ghi được thực hiện. Một trong số đó là công cụ kiểm chứng Yogar-CBMC, sử dụng kiến trúc hình cây EOG. Công cụ cho kết quả tốt trên bộ thực nghiệm của cuộc thi SV-COMP 2017 [1]. Tuy nhiên, với chương trình có một số lượng lớn các điểm xung đột đọc / ghi phức tạp, phương pháp Yogar-CBMC cho hiệu quả không cao do phải thực thi nhiều vòng lặp. Vấn đề này có thể giải quyết bằng phương pháp kết hợp EOG và kỹ thuật thực thi tượng trưng để sinh ràng buộc cho toàn bộ các tín hiệu đọc / ghi chỉ trong một vòng lặp. Kỹ thuật thực thi tượng trưng sẽ tạo ra AST và CFG từ đoạn mã của chương trình. Sau đó, dựa trên CFG, các đỉnh trên EOG được tạo ra và từ đó sinh ra các ràng buộc đọc / ghi để tránh việc xung đột.

# **Chương 2. Kiểm chứng dựa trên kỹ thuật thực thi tượng trưng**

* 1. **Kỹ thuật thực thi tượng trưng**
     1. **Khái niệm**

Thực thi tượng trưng (symbolic execution) là một kỹ thuật trong lĩnh vực kiểm thử phần mềm, cho phép tự động tìm kiếm các lỗi trong mã nguồn của chương trình bằng cách phân tích các đường đi có thể của chương trình dựa trên các biểu thức và ràng buộc logic.

Ý tưởng chính của thực thi tượng trưng là thay thế việc sử dụng tham số đầu vào là các giá trị cụ thể (concrete value) bằng các giá trị tượng trưng (symbolic value), khi đó đầu ra sẽ được tính toán dựa trên các giá trị tượng trưng này và được biểu diễn dưới dạng một biểu thức tượng trưng.

Lấy ví dụ với câu lệnh sau:

***if a then b else c***,

Đối với việc sử dụng tham số đầu vào là các giá trị cụ thể, chỉ có duy nhất một luồng điều khiển được thực thi. Mỗi một lần thực thi cụ thể, luồng điều khiển chỉ có thể rẽ vào một trong hai nhánh ***b*** hoặc ***c***, tùy theo giá trị cụ thể của ***a***. Vì vậy, trong hầu hết các trường hợp, thực thi cụ thể chỉ có thể đánh giá tương đối độ thỏa mãn của chương trình với đặc tả yêu cầu.

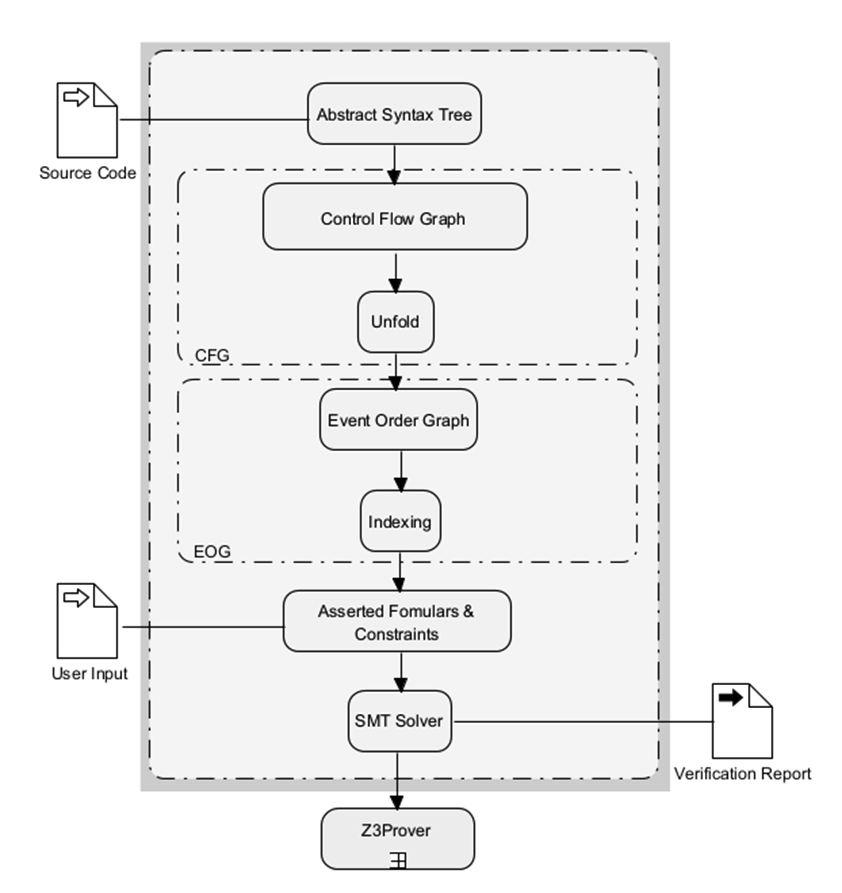
Ngược lại, đối với thực thi tượng trưng, việc đi theo nhánh ***b*** hay ***c*** không được cố định vì ***a*** không phải là một cụ thể. Tại điểm rẽ nhánh ***a***, cả hai nhánh ***b*** và ***c*** cùng đồng thời được xem xét nhằm định hướng cho bước kế tiếp của luồng điều khiển, do đó nó đảm bảo tất cả các luồng điều khiển của chương trình đều được kiểm tra một cách đầy đủ và chính xác.

Thực thi tượng trưng có hai hướng tiếp cận: thực thi tượng trưng động – Dynamic symbolic execution DSE và thực thi tượng trưng tĩnh – Static symbolic execution SSE. DSE tạo ra công thức của từng đường đi và kiểm tra từng đường thực thi cụ thể trong khi SSE tạo ra công thức của đường đi của cả chương trình trước khi kiểm tra các đường thực thi. Có thể nhận thấy rằng, SSE sẽ có lợi thế hơn trong việc kiểm chứng, đặc biệt là kiểm chứng các chương trình lớn vì nó ít bị ảnh hưởng bởi bùng nổ đường thực thi. Tuy nhiên, SSE sẽ gặp phải rất nhiều các vấn đề liên quan đến giá trị động như xử lý vòng lặp và đệ quy do số lượng vòng lặp và số lần đệ quy chỉ được xác định trong trạng thái runtime.

Tài liệu nghiên cứu này sẽ đi sâu vào phân tích kiểm chứng chương trình đa luồng theo hướng thực thi tượng trưng tĩnh SSE.

* + 1. **Kiến trúc thực thi tượng trưng trong kiểm chứng chương trình đa luồng**

Phương pháp kiểm chứng này nhận dữ liệu đầu vào gồm hai thành phần: mã nguồn của chương trình và điều kiện kiểm chứng của người dùng, kết quả đầu ra là một bản báo cáo hoạt động của công cụ về kết quả kiểm chứng của chương trình tương ứng với điều kiện đầu vào của người dùng.



Hình 2.1.3.1. Kiến trúc thực thi tượng trưng

Sau khi có được mã nguồn của chương trình, công cụ kiểm chứng sẽ tiến hành trừu tượng hóa chương trình dựa trên kĩ thuật thực thi tượng trưng. Mã nguồn sẽ được đưa vào bộ phiên dịch ngôn ngữ của máy tính để tạo nên cây cú pháp trừu tượng AST biểu diễn cấu trúc cú pháp của mã nguồn. Trên cơ sở cấu trúc cú pháp được biểu diễn trong AST, đồ thị luồng điều khiển CFG biểu diễn các luồng điều khiển được sinh ra. CFG tiếp đến sẽ được trải phẳng bằng cách thay thế các đoạn mã vòng lặp/đệ quy bằng khối lệnh tuyến tính với độ dài giới hạn. Từ luồng điều khiển, các hành động đọc / ghi sẽ được lọc ra để tạo ra đồ thị thứ tự sự kiện EOG, mỗi một hành động là một đỉnh trong EOG. Các đỉnh này được đánh chỉ số để có thể trừu tượng hóa bằng các logic vị từ cấp một . Tại đây, trừu tượng này sẽ được kết hợp với điều kiện kiểm chứng trước khi đưa vào bộ giải SMT. Báo cáo hoạt động của công cụ sẽ được xuất ra sau khi bộ giải SMT trả về kết quả.

Báo cáo hoạt động của công cụ sẽ đưa ra kết quả của việc chạy chương trình, có thể nhận được các kết quả sau:

* UNSATISFIABLE: điều kiện đặt lên chương trình luôn đúng.
* SATISFIABLE: điều kiện sai trong một số trường hợp, kèm theo đó là counter example của trường hợp đó.
  + 1. **Trừu tượng hóa trong thực thi tượng trưng**

*Một vấn đề mà phần lớn các chương trình kiểm chứng đều mắc phải, điển hình là các công cụ kiểm chứng dựa trên kỹ thuật kiểm chứng mô hình đó là việc bùng nổ số trạng thái. Việc áp dụng phương pháp thực thi tượng trưng để trừu tượng hóa chương trình vào kiểm chứng sẽ giúp giảm thiểu nguy cơ bùng nổ trạng thái, từ đó có thể sử dụng để kiểm chứng cho các hệ thống lớn và phức tạp.*

*Thay vì biểu diễn cụ thể từng đường thi hành, chương trình sẽ được tổng quát hóa thành các biểu thức logic vị từ cấp một. Các biểu thức logic sinh ra sẽ được sử dụng để phân tích, kiểm tra mã nguồn và sự thỏa mãn của chương trình với các điều kiện được đặc tả bởi người dùng.*

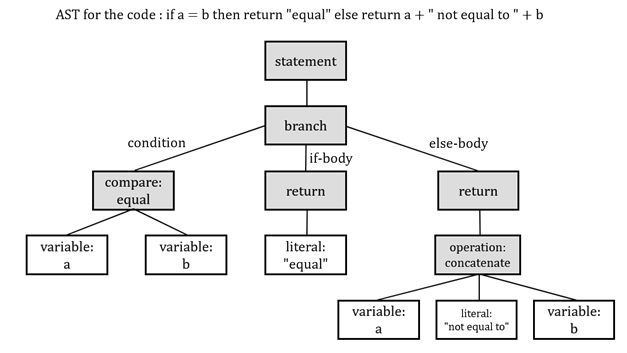
*Phần này sẽ trình bày về việc trừu tượng hóa chương trình nhằm mục đích sinh ra cây cú pháp trừu tượng AST và đồ thị luồng điều khiển CFG. Việc xây dựng đồ thị thứ tự sự kiện EOG từ CFG và tổng quát hóa EOG thành các biểu thức logic vị từ cấp một sẽ được trình bày trong các phần sau.*

* + - 1. **Abstract Syntax Tree**

Abstract syntax tree (AST) là một cấu trúc dữ liệu phân cấp biểu diễn cú pháp trừu tượng của một đoạn mã (code) trong một ngôn ngữ lập trình nhất định. Nó được sử dụng như một công cụ phân tích cú pháp (parser) trong quá trình biên dịch hoặc thông dịch mã nguồn.

AST thường được tạo ra bằng cách duyệt cây cú pháp của một đoạn mã và tạo ra các đối tượng phân tích cú pháp (parse nodes) biểu diễn cho mỗi phần của cú pháp. Các đối tượng này được sắp xếp theo thứ tự phân cấp tương ứng với cấu trúc cú pháp của đoạn mã.

AST thường được sử dụng trong các công cụ phân tích mã nguồn như trình biên dịch hoặc trình thông dịch để thực hiện các tác vụ phân tích mã như tối ưu hóa, dò lỗi, tạo mã trung gian, hoặc thậm chí là tự động sinh mã.



Hình 2.2.1.1. Abstract Syntax Tree của một khối lệnh đơn giản

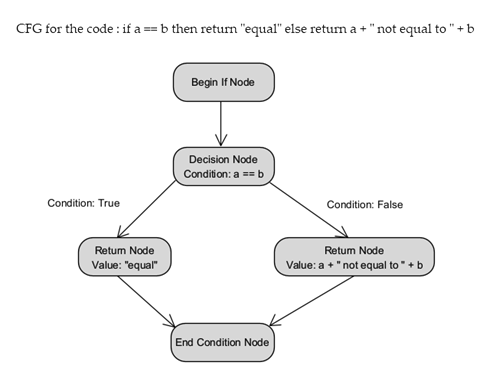
* + - 1. **Control Flow Graph**

Control flow graph (CFG) là một biểu đồ đồ họa thể hiện luồng điều khiển hoặc luồng thực thi của một chương trình máy tính. Nó được sử dụng để trực quan hóa cách chương trình thực thi và phân tích hành vi của nó.

Biểu đồ CFG bao gồm các đỉnh và cạnh. Các đỉnh đại diện cho các khối cơ bản của mã lệnh thực hiện một chuỗi các hoạt động mà không có bất kỳ thay đổi luồng điều khiển nào, trong khi các cạnh đại diện cho luồng điều khiển giữa các đỉnh. Một cạnh có thể đại diện cho một điểm quyết định trong mã lệnh, chẳng hạn như một câu lệnh if-else hoặc vòng lặp, hoặc nó có thể đại diện cho một dòng lệnh thực thi thẳng.

Trong nghiên cứu này, CFG sẽ được phân tích từ AST xây dựng dựa trên mã lệnh, các khối cơ bản của mã lệnh sẽ là các đỉnh nằm trên AST. Mỗi khối cơ bản được đại diện bởi một đỉnh trong biểu đồ CFG, và các câu lệnh điều khiển được đại diện bởi các cạnh.

CFG là một công cụ hữu ích cho phân tích chương trình, tối ưu hóa và kiểm tra. Nó có thể được sử dụng để xác định các lỗi tiềm ẩn, xác định thời gian thực thi của chương trình, tối ưu hóa chương trình bằng cách xác định các điểm nóng, và tạo ra các trường hợp kiểm tra bao phủ tất cả các đường đi thực thi có thể. CFG cũng có thể biểu thị rõ ràng cấu trúc và hành vi của mã, làm cho việc bảo trì và sửa đổi mã dễ dàng hơn.



Hình 2.2.2.1. Control Flow Graph của một khối lệnh đơn giản

* 1. **Satisfiability Modulo Theories**

Sau khi chương trình được trừu tượng hóa thành các biểu thức vị từ cấp một, Satisfiability Modulo Theories sẽ được sử dụng để kiểm tra tính đúng đắn của tập các biểu thức vị từ cấp một đó.

Satisfiability Modulo Theories (SMT) là một phương pháp giải quyết bài toán logic được sử dụng trong lĩnh vực máy tính và khoa học máy tính. SMT kết hợp sự mạnh mẽ của việc tự động chứng minh định lý trong logic và kỹ thuật giải quyết bài toán tìm kiếm cục bộ để giải quyết bài toán liên quan đến hệ thống các giả thiết liên quan đến các lý thuyết khác nhau.

Cụ thể, SMT tập trung vào việc xác định tính khả thi của một tập hợp các ràng buộc logic trong khi đồng thời sử dụng các giả thiết từ các lý thuyết khác nhau. Các lý thuyết này có thể bao gồm cả số học, giải tích, lý thuyết tập hợp, lý thuyết chuỗi, lý thuyết mảng, lý thuyết đồng thời và nhiều lý thuyết khác nữa.

Bộ giải SMT giúp người dùng dễ dàng có thể hình dung được xu hướng di chuyển vào các nhánh trong quá trình thực hiện chương trình, mô hình hóa các biểu thức điều kiện, số học và mảng. Bằng cách thêm vào những điều kiện khác nhau, người dùng có thể sử dụng bộ giải SMT để đưa các điều kiện này vào những nhánh thi hành khác nhau của chương trình, đảm bảo vị trí lưu trữ luôn có một giá trị cụ thể và kiểm tra các điều kiện.

# **Chương 3. Xây dựng phương pháp kiểm chứng chương trình đa luồng ACIO**

## Kiểm chứng dựa trên đồ thị thứ tự sự kiện EOG

*Nội dung phần này có tham khảo, sử dụng các định nghĩa, phương pháp và kết quả của nghiên cứu được trình bày trong tài liệu Scheduling Constraint Based Abstraction Refinement for Multi-Threaded Program Verification* [2] *của nhóm tác giả Liangze Yin, Wei Dong, Wanwei Liu và Ji Wang đến từ School of Computer, National University of Defense Technology, China kết hợp với các nghiên cứu cơ sở của các nhóm tác giả khác.*

* + 1. **Multi-threaded Program**

Nghiên cứu này sẽ tập trung vào kiểm chứng chương trình C/C++ sử dụng Pthread, một trong những thư viện phổ biến nhất trong lập trình đa luồng. Thư viện Pthread sử dụng pthread\_create(&t, &attrib, &f, &args) để bắt đầu chạy luồng t và pthread\_join(t, &return) để tạm dừng luồng hiện tại cho đến khi luồng t hoàn tất thực thi.

Một chương trình đa luồng P có N luồng P­i ­ (N ≥ 1, 1 ≤ i ≤ N) đồng thời chạy song song với nhau. P có một tập các biến được chia thành hai nhóm: biến toàn cục và biến cục bộ. Mỗi luồng P­­­­­i có thể đọc/ghi biến toàn cục và biến cục bộ của nó.

*Giả định rằng toàn bộ các biến trong P là nguyên tử, đồng thời toàn bộ các vòng lặp / đệ quy có chiều sâu là giới hạn (điều kiện cơ bản trong Bounded Model Checking, sẽ đượng trình bày trong mục* ***2.3.2. Bounded Model Checking****). Ngoài ra, việc mô hình hóa các cấu trúc dữ liệu phức tạp như là con trỏ, cấu trúc, mảng... các phép tính và ký pháp phép tính phức tạp như là lũy thừa, logarit, ++, --... và một số hàm của Pthread như pthread\_mutex\_lock, pthread\_mutex\_unlock sẽ bị bỏ qua trong nghiên cứu này.*

Chương trình đa luồng P có V là tập các biến toàn cục. E là tập các sự kiện e biểu thị một hành động đọc hoặc ghi vào một biến toàn cục. Mỗi sự kiện e tương ứng với một phần tử biến var(e) ∈ V, một kiểu hành động type(e) (type(e) = read nếu sự kiện e biểu thị cho hành động đọc và type(e) = write nếu sự kiện e biểu thị cho hành động ghi) và một giá trị value(e) là giá trị được thao tác trên var(e).

**Định nghĩa** là một tập hợp các cặp gồm 2 sự kiện (ei, ej) với ei ⊂ E và ej ⊂ E (*hay ⊂ E × E*). Mỗi một cặp sự kiện (ei, ej) ∈ (*hay ei  ej*) biểu thị rằng “sự kiện ei sẽ xảy ra trước sự kiện ej trong luồng thực thi chương trình P”.

**Định nghĩa** là một tập hợp các cặp gồm 2 sự kiện (ei, ej) với ei ⊂ E và ej ⊂ E (*hay ⊂ E × E*). Mỗi một cặp sự kiện (ei, ej) ∈ (*hay ei  ej*) biểu thị rằng “sự kiện ei sẽ xảy ra trước sự kiện ej trong luồng thực thi chương trình P, dựa trên mã nguồn của P”. Nếu ei ej thì ei  ej, hay nói cách khác ⊂ . Một cặp sự kiện (ei, ej) ∈ có thể được tạo ra từ các trường hợp sau:

* Với hai sự kiện ei và ej trong cùng một luồng, nếu ei xảy ra trước ej dựa trên thứ tự câu lệnh trong mã nguồn thì ei ej.
* Nếu pthread\_create() được dùng để tạo một luồng t tại một điểm p trong luồng hiện tại, với mọi sự kiện ei xảy ra trước p trong luồng hiện tại và mọi sự kiện ej trong luồng t thì ei ej.
* Nếu pthread\_join() được dùng để tạm dừng luồng hiện tại tại thời điểm p để đợi luồng t thực thi xong, với mọi sự kiện ei trong luồng t và mọi sự kiện ej xảy ra sau p trong luồng hiện tại thì ei ej.

**Định nghĩa** liên kết đọc-ghi S(ei, ej) biểu thị rằng “hành động đọc ej sẽ đọc được giá trị ghi bởi hành động ghi ei”. Điều đó có nghĩa là ei ej, type(ej) == read, type(ei) == write, var(ej) == var(ei) và value(ej) == value(ei). Thêm vào đó, nếu S(ei, ej) tồn tại thì với mọi hành động ghi ek ≠ ei:

* S(ek, ej) không tồn tại. Nói cách khác, nếu ej đọc được giá trị ghi vào bởi ei, ej sẽ không thể đọc được giá trị ghi vào bởi ek. Điều đó đảm bảo hành động đọc sẽ trả về kết quả là duy nhất.
* ek ei hoặc ej ek. Nếu vẫn tồn tại ek thỏa mãn ei ek ej thì khi đó, tuy rằng var(ei) == var(ej) = var nhưng value(ei) ≠ value(ej) do var đã bị ghi đè giá trị của hành động ghi ek, hay value(ek) = value(ej). Do đó S(ei, ej) là không tồn tại. Điều đó phủ định lại giả thuyết S(ei, ej) được đặt ra ban đầu.

Mỗi liên kết đọc-ghi sẽ được biểu thị bằng một biến boolean nhận giá trị true/false gọi là chữ ký (signature). Chữ ký của liên kết đọc-ghi có giá trị là true nếu liên kết đọc-ghi đó có tồn tại, ngược lại sẽ có giá trị là false.

* + 1. **Bounded Model Checking**

Bounded model checking [3] là một trong những kỹ thuật được áp dụng nhiều nhất để giảm thiểu vấn đề bùng nổ không gian trạng thái trong kiểm định chương trình đa luồng. Cho rằng hầu hết các lỗi có thể xác định với một số lượng giới hạn các vòng lặp, khi đó các vòng lặp/vòng đệ quy có thể được trải phẳng thành các đoạn mã tuyến tính với độ dài giới hạn [4]. Thay vì liệt kê rõ ràng toàn bộ các xen kẽ luồng, BMC sử dụng biểu tượng để thể hiện cho việc mã hóa vấn đề kiểm chứng, thứ sẽ được giải bằng một bộ giải SMT. Nếu bộ giải SMT cho kết quả là SAT thì chương trình có luồng điều khiển tương ứng với phản ví dụ counter example (nói cách khác là cách mà chương trình thực thi để vi phạm điều kiện kiểm chứng). Nếu kết quả là UNSAT thì chương trình được chứng minh là thỏa mãn điều kiện kiểm chứng với số lượng giới hạn các vòng lặp được đặt ra.

Trong BMC, kiến trúc trừu tượng của một chương trình đa luồng thường được thể hiện dưới dạng

**α := ϕinit ∧ ρ ∧ ζ ∧ ξ**

trong đó, ϕinit là các trạng thái khởi đầu của chương trình, ρ mã hóa từng luồng một cách riêng biệt với nhau, ζ biểu thị cho ràng buộc “mỗi hành vi đọc trên một biến v có thể đọc được giá trị được ghi bởi bất kì hành vi ghi trên biến v khả thi” và ξ biểu thị cho ràng buộc “với mỗi cặp ⟨w, r⟩, hành động đọc r đọc được giá trị của biến v được ghi bởi hành động ghi w, ngoài ra các hành động ghi khác nằm giữa chúng không có bất kì hành động ghi trên biến v nào” [5].

* + 1. **Đồ thị thứ tự sự kiện**
       1. **Phản ví dụ**

**Định nghĩa:** Phản ví dụ π của kiến trúc trừu tượng α là tập hợp các phép gán cho các biến trong α ∧ ϕerr, với ϕerr là các trạng thái lỗi cần kiểm chứng.

Phản ví dụ π là một trình tự thực thi của trừu tượng α mà vi phạm điều kiện kiểm chứng. Nó định nghĩa đường thực thi cho từng luồng và mối quan hệ đọc-ghi giữa các hành động đọc và ghi xảy ra trong π.

Một phản ví dụ π là một tập hợp gồm 4 thành phần ⟨S0,π, Eπ,, £π⟩, trong đó S0,π là điều kiện khởi đầu của π,Eπ là tập hợp các sự kiện trong π, là mối quan hệ giữa các sự kiện ghi và đọc (tức là các phép gán giá trị) dựa trên mã nguồn chương trình và £π là tập hợp các liên kết đọc-ghi trong π.

Một chương trình có thể không có, có một hoặc có nhiều phản ví dụ, tùy vào số lượng trình tự thực thi vi phạm điều kiện kiểm chứng mà nó sở hữu.

* + - 1. **Xây dựng đồ thị thứ tự sự kiện EOG**
         1. Định nghĩa đồ thị thứ tự sự kiện EOG

Cho một phản ví dụ π, đồ thị thứ tự sự kiện Gπ là một tập hợp gồm 3 thành phần ⟨Eπ, , £π⟩. Các đỉnh trong Gπ được định nghĩa bởi Eπ và các cạnh trong Gπ được định nghĩa bởi và £π.

Mỗi một đỉnh tương ứng với một trong hai hành động đọc và ghi.

Mỗi một cạnh được định nghĩa bởi nối đỉnh thứ nhất n1 với đỉnh thứ hai n2, đảm bảo rằng n1 n2 .

Mỗi một cạnh được định nghĩa bởi £π nối đỉnh thứ nhất n1 với đỉnh thứ hai n2, đảm bảo rằng n1 *n2*, var(n1) = var(n2), type(n1) = write, type(n2) = read, value(n1) = value(n2), giữa chúng không có bất kì đỉnh nào ghi giá trị vào biến v và không có bất kì cạnh nào khác được định nghĩa bởi £π có đỉnh thứ hai là n2.

* + - * 1. Kiến trúc của đồ thị thứ tự sự kiện EOG

EOG là một đồ thị gồm nhiều đỉnh có liên kết với nhau, mỗi đỉnh đồng thời phải thỏa mãn các điều kiện sau:

* *Mỗi một đỉnh biểu diễn duy nhất một hành động trong hai hành động đọc và ghi.*
* *Mỗi một đỉnh phải tham chiếu đến duy nhất một biến, là đối tượng của hành động đọc/ghi tại đỉnh đó (gọi tắt là đỉnh đọc / đỉnh ghi)*
* *Mỗi một đỉnh đều có liên kết đến các đỉnh trước nó dựa trên thứ tự thể hiện trong mã nguồn. Số lượng liên kết có thể là 0 với đỉnh bắt đầu, 1 với các đỉnh nằm trong khối lệnh tuyến tính và nhiều hơn 1 với các đỉnh mà đoạn mã tương ứng của nó trong mã nguồn nằm ngay sau lệnh pthread\_join.*
* *Mỗi một đỉnh đều có liên kết đến các đỉnh sau nó dựa trên thứ tự thể hiện trong mã nguồn. Số lượng liên kết có thể là 0 với đỉnh kết thúc, 1 với các đỉnh nằm trong khối lệnh tuyến tính và nhiều hơn 1 với các đỉnh mà đoạn mã tương ứng của nó trong mã nguồn nằm ngay trước lệnh pthread\_create.*

## Phương pháp biểu diễn ràng buộc

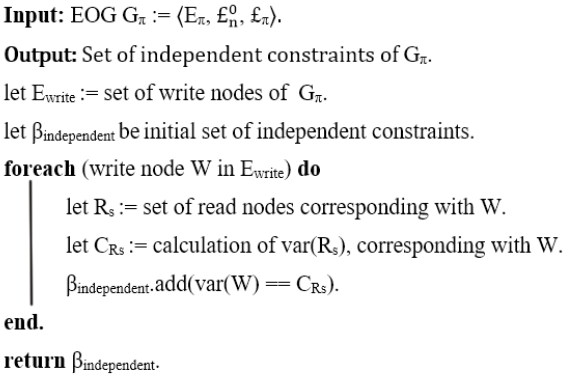
*Với đồ thị thứ tự sự kiện Gπ = ⟨Eπ, , £π⟩, các ràng buộc sẽ được xây dựng dựa trên các cạnh của Gπ, hay nói cách khác là dựa trên các phép gán giá trị và các liên kết đọc-ghi £π.*

* + 1. **Ràng buộc độc lập trên các luồng**

Ràng buộc độc lập trên các luồng (gọi tắt là ràng buộc độc lập) là ràng buộc được xây dựng dựa trên quá trình đọc giá trị từ tập các biến ri, thực hiện tính toán trên tập biến này rồi ghi kết quả vào một biến wi nào đó, hay nói cách khác là dựa trên các phép gán giá trị. Ràng buộc này được gọi là độc lập giữa các luồng vì mỗi một phép gán giá trị chỉ nằm trong một luồng duy nhất, không ảnh hưởng tới các luồng còn lại. Do đó nó sẽ được biểu thị bằng phép gán giá trị tương ứng (kèm thêm chỉ số).

Ví dụ: *y = x + z → y1 = x2 + z3*

Các điều kiện khởi đầu nhìn chung cũng là một phép gán giá trị, do đó việc mã hóa chúng cũng tương tự như trên.

****Ví dụ: *y = 0 → y0 = 0*

**Algorithm 1. Independent constraints generation.**

* + 1. **Ràng buộc cho các biến đọc/ghi dữ liệu**

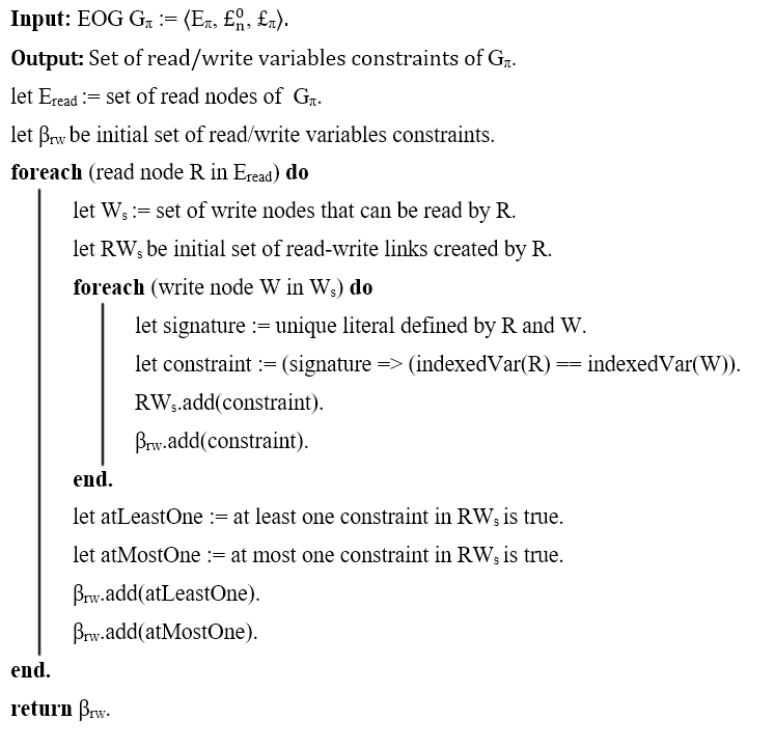
Ràng buộc cho các biến đọc/ghi (gọi tắt là ràng buộc đọc-ghi) là ràng buộc được tạo nên bởi một hành động đọc và nhiều hành động ghi. Ràng buộc đọc-ghi biểu thị rằng với mỗi một hành động đọc, nó có thể đọc được giá trị ghi bởi bất kì các hành động ghi khả thi, đồng thời chỉ có thể đọc được duy nhất giá trị ghi bởi hành động ghi đó. Điều đó có nghĩa là ràng buộc đọc ghi đảm bảo hành động đọc đọc được giá trị là duy nhất.

Cho rằng {r0}là tập các hành động đọc, {w0, w1, w2} là tập các hành động ghi. Cả hai tập hành động này cũng thao tác lên một biến x nào đó. Khi đó:

* r0 có thể đọc được giá trị ghi bởi w0, w1 hoặc w2.

**(***S(r0, w0) → r0 = w0***)** **∧ (***S(r0, w1) → r0 = w1***) ∧ (***S(r0, w2) → r0 = w2***)**

* r0 có thể đọc được một và chỉ một giá trị ghi bởi w0, w1 hoặc w2

****at\_least(***S(r0, w0), S(r0, w1), S(r0, w2)***)** **∧ at\_most(***S(r0, w0), S(r0, w1), S(r0, w2)***)****Algorithm 2. Read/write variables constraints generation.**

* + 1. **Ràng buộc đảm bảo thứ tự thực thi**

*Điểm quan trọng trong cách trừu tượng hóa chương trình của phương pháp ACIO là việc suy diễn các ràng buộc để đảm bảo thứ tự thực thi dựa trên các liên kết đọc-ghi. Ràng buộc đảm bảo thứ tự thực thi phát biểu rằng tính đúng đắn của liên kết đọc-ghi này sẽ phủ nhận tính đúng đắn của một số liên kết đọc-ghi khác để chắc chắn rằng các biến đọc không đọc được các giá trị chưa hề được ghi hoặc đã bị ghi đè bởi biến ghi khác.*

* 1. **Minh họa phương pháp**
  2. **Đánh giá với phương pháp đã có**

# **Chương 4. Thực nghiệm đánh giá**

# **Kết luận**

# **Tài liệu tham khảo**

|  |  |
| --- | --- |
| [1] | S.-C. 2017, “SV-COMP 2017 - 6th International Competition on Software Verification (sosy-lab.org),” 2017. [Trực tuyến]. Available: https://sv-comp.sosy-lab.org/2017/results/results-verified/. |
| [2] | Liangze Yin, Wei Dong, Wanwei Liu, Ji Wang, “Scheduling Constraint Based Abstraction Refinement forMulti-Threaded Program Verification,” [Trực tuyến]. Available: https://www.researchgate.net/publication/319326871\_Scheduling\_Constraint\_Based\_Abstraction\_Refinement\_for\_Multi-Threaded\_Program\_Verification. |
| [3] | Armin Biere, Alessandro Cimatti, Edmund M. Clarke, Yunshan Zhu, “Symbolic Model Checking without BDDs,” trong *International Conference on Tools and Algorithms for Construction and Analysis of Systems*, 1999, pp. 193-207. |
| [4] | Shaz Qadeer, Jakob Rehof, “Context-Bounded Model Checking of Concurrent Software,” trong *International Conference on Tools and Algorithms for Construction and Analysis of Systems*, 2005, pp. 93-107. |
| [5] | Jade Alglave, Daniel Kroening, Michael Tautschnig, “Partial Orders for Efficient Bounded Model Checking of Concurrent Software,” trong *International Conference on Computer Aided Verification*, 2013, pp. 141-157. |