ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

Trương Xuân Hiếu

PHÂN TÍCH TĨNH CHƯƠNG TRÌNH ĐA LUỒNG

KHÓA LUẬN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành Công nghệ thông tin

Cán bộ 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 tới các anh chị và các bạn, đặc biết là tập thể lớp QH-2019-I/CQ-C-D 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

Em xin cam đoan rằng những nghiên cứu về phương pháp phân tích tĩnh chương trình đa luồng được trình bày trong khóa luận này là của em 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 em viết ra không sao chép từ các tài liệu, không sử dụng các kết quả của người khác mà không trích dẫn cụ thể. Em xin cam đoan cốt lõi của phương pháp mã hóa sinh ràng buộc được sử dụng trong công cụ được trình bày trong khoá luận là do em tự phát triển, không sao chép mã nguồn của người khác.

Nếu sai em 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

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 khá phức tạp trong việc xác định trình tự thực thi vì câu lệnh của các luồng trong chương trình chạy đan xen (interleave) vào nhau không theo một trình 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 thế cho các phương pháp kiểm thử truyền thống. Phương pháp kiểm chứng này 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. Diễn giải chi tiết về phương pháp kiểm chứng ACIO sẽ được trình bày chi tiết trong tài liệu này.

Từ khóa: *Kiểm chứng, đa luồng, Event Order Graph, thực thi tượng trưng.*

DANH SÁCH KÍ HIỆU

- **ACIO** All-Conflicts-In-One
- **AST** Abstract Syntax Tree
- **CFG** Control Flow Graph
- **EOG** Event Order Graph
- **SMT** Satifiability Modulo Theories
- **SV-COMP** Software Verification Competition

DANH SÁCH BẢNG BIỂU

DANH SÁCH HÌNH VẼ

CHƯƠNG 1. KIỂM CHỨNG CHƯƠNG TRÌNH ĐA LUỒNG

1.1. 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 phổ biến. Tuy nhiên, các đầu vào cụ thể 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. Việc kiểm thử thiếu các đầu vào ít phổ biến hơn có thể dẫn đến việc bỏ sót nhiều lỗi của chương trình, làm ảnh hưởng đến kết quả 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.

1.1.1. Kiểm chứng chương trình

Kiểm chứng chương trình (software verification) là quy trình xác minh xem chương trình hoạt động đúng như mong đợi hay không. Trong quy 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.

1.1.2. Kiểm chứng mô hình

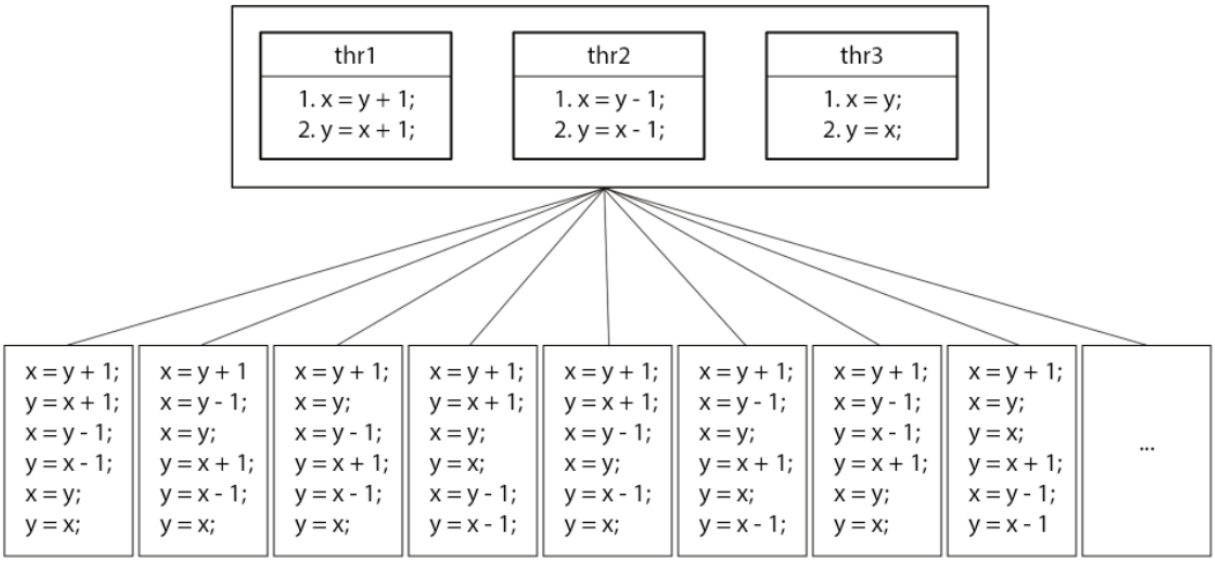
Trong thực tế thiết kế và phát triển phần mềm, công việc kiểm chứng tiêu tốn nhiều thời gian và công sức hơn là việc xây dựng hệ thống. Do đó, nhu cầu tìm kiếm một kỹ thuật kiểm chứng hiệu quả và giảm thiểu tối đa chi phí đang ngày càng trở nên cấp thiết. Một trong những kỹ thuật kiểm chứng cho hiệu quả cao có thể kể đến là kỹ thuật kiểm chứng mô hình.

Kỹ thuật kiểm chứng mô hình là quy trình sử dụng các phương pháp, công cụ và kỹ thuật mô hình hóa 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 bằng các công thức toán học. 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.

1.2. Thực thi đa luồng

Trong kiểm chứng chương trình, thực thi đa luồng là một trong những vấn đề thách thức nhất. Về mặt lý thuyết, các luồng trong chương trình được thực thi một cách “song song”. Tuy nhiên trong thực tế, các câu lệnh trong các luồng sẽ đan xen vào nhau theo một thứ tự không cố định. Việc đan xen không theo thứ tự cố định này khiến việc xác định trình tự thực thi vô cùng phức tạp. Do đó, kiểm chứng bằng việc xây dựng các trình tự thực thi dựa trên quy trình xen kẽ các câu lệnh và thực thi lần lượt là không hề đơn giản, chưa kể đến độ phức tạp của chính bản thân các câu lệnh đó.



Hình 1. Một số trình tự thực thi của chương trình đa luồng

Xét một chương trình đơn giản chỉ gồm ba luồng chạy song song *thr1, thr2 và thr3,* mỗi luồng bao gồm hai câu lệnh gán giá trị như trên *Hình 1. Một số trình tự thực thi của chương trình* Giả thiết rằng dòng lệnh *thr1.1* sẽ được thực thi đầu tiên, khi đó tập các dòng lệnh tiếp theo có thể được thực thi là *{thr1.2, thr2.1, th3.1}.* Nếu trong ba dòng lệnh đó, *thr2.1* được chọn để thực thi thì tập các dòng lệnh tiếp theo có thể được thực thi sẽ trở thành *{thr1.2, thr2.2, th3.1}*. Tổng quát hơn, mỗi khi một dòng lệnh trong một luồng được thực thi, luồng điều khiển có thể tiếp tục thực thi dòng lệnh tiếp theo trong cùng luồng hoặc chuyển sang thực thi các luồng còn lại. Nói cách khác, với chương trình có *n* luồng, mỗi bước lựa chọn dòng lệnh thực thi tiếp theo sẽ có tối đa *n* lựa chọn. Cho rằng mỗi luồng trong chương trình đó có *m* dòng lệnh, tức là toàn bộ chương trình sẽ có *m*n* dòng lệnh, đồng thời coi các trường hợp đặc biệt (bước lựa chọn dòng lệnh thực thi tiếp theo có ít hơn n lựa chọn) cũng có n lựa chọn, việc xác định trình tự thực thi của chương trình sẽ là *m*n* lần chọn *1* trong *n* khả năng khả thi. Điều đó có nghĩa là một chương trình *n* luồng song song, mỗi luồng có *m* dòng lệnh ước tính sẽ có n^{m*n} trình tự thực thi khác nhau đôi một.

Công thức trên có sai số khá lớn khi áp dụng vào ví dụ trong *Hình 1* với $3^{2*3} = 729$ luồng thực thi trên tính toán và chỉ 90 luồng thực thi trong thực tế, tỉ lệ sai số 8100%. Nguyên nhân là do các luồng trong chương trình chỉ bao gồm hai câu lệnh khiến các trường hợp đặc biệt chiếm đa số. Dù vậy, có thể thấy rằng 729 hay 90 đều là một con số tương đối lớn so với con số 6 của tổng số dòng lệnh.

Đối với chương trình có các luồng lớn phức tạp yêu cầu nhiều thao tác đọc/ghi hơn, tỉ lệ sai số sẽ giảm đi do tỉ lệ trường hợp đặc biệt được giảm thiểu, tuy nhiên việc sai số vẫn là không thể tránh khỏi. Do đó, công thức trên không có giá trị trong việc định lượng mà chỉ có giá trị trong việc định tính mức độ phức tạp của việc xác định luồng thực thi.

1.3. Kiểm chứng thực thi đa luồng

Bởi sự phức tạp trong việc kiểm chứng chương trình đa luồng, đã có rất nhiều diễn đàn được mở ra để phân tích các thách thức và đồng thời thảo luận về phương pháp giải quyết. Một trong những diễn đàn có thể kể đến là cuộc thi SV-COMP [9]. Cuộc thi được tổ chức bởi trường đại học Ludwig Maximilians, Munich, Đức. Mục tiêu của cuộc thi là tìm ra giải pháp tốt nhất cho việc kiểm chứng chương trình đa luồng. Các đội tham dự cần xây dựng công cụ để kiểm chứng các chương trình mẫu cho trước (Benchmark). Kết quả của từng đội sẽ được đánh giá và cho điểm dựa trên rất nhiều thang đo khác nhau như ReachSafety, MemorySafety, ConcurrencySafety... trước khi được tổng kết và xếp hạng. Công cụ được sử dụng trong nghiên cứu này cũng sẽ được thực nghiệm đánh giá dựa trên Benchmark của cuộc thi SV-COMP.

Một trong những cách rất hiệu quả trong việc kiểm chứng chương trình đa luồng được các đội tham dự thi đấu sử dụng đó là mã hóa các tín hiệu đọc / ghi giá trị để kiểm tra xung đột. Một chương trình dù đơn giản hay phức tạp thì dưới sự ghi nhận của bộ nhớ máy tính, chương trình đó cũng chỉ đơn thuần đọc giá trị từ các ô nhớ, thao tác với các giá trị đọc được rồi ghi lại giá trị vào một số ô nhớ nào đó. Do đó, việc mã hóa tín hiệu đọc/ghi không chỉ đảm bảo mã hóa đủ thông tin cần thiết mà còn đảm bảo không mã hóa các thông tin dư thừa Ngoài ra, việc kiểm tra xung đột giữa các tín hiệu đọc/ghi còn đơn giản hơn rất nhiều do tập phần tử của chúng chỉ bao gồm hai phần tử đọc và ghi.

Một trong số nghiên cứu đạt thành tích cao trong cuộc thi SV-COMP sử dụng việc mã hóa các tín hiệu đọc/ghi là công cụ kiểm chứng Yogar-CBMC, sử dụng kiến trúc đồ thị EOG. Công cụ cho kết quả tốt trên bộ thực nghiệm của cuộc thi SV-COMP 2017 [10] với việc kiểm chứng đúng 1047 chương trình đa luồng trong thời gian giới hạn với điểm số cao nhất đạt được là 1293. Tuy nhiên, do phương pháp Yogar-CBMC được chia thành nhiều vòng lặp (iterators), mỗi vòng lặp chỉ mã hóa một phần các tín hiệu đọc / ghi để bổ sung vào tập ràng buộc của vòng lặp trước (tức là tập ràng buộc của vòng lặp sau bao hàm tập ràng buộc của vòng lặp trước) rồi đưa vào bộ giải SMT để tìm ra phản ví dụ. Bộ giải SMT

lúc này sẽ phải tiêu tốn một lượng lớn thời gian để giải các tập ràng buộc tương đồng, đặc biệt là đối với các chương trình phức tạp yêu cầu nhiều vòng lặp.

Trong nghiên cứu này, em đề xuất 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 duy nhất. Việc chỉ sử dụng một vòng lặp để sinh ràng buộc vừa có thể giúp bộ giải SMT có thể đồng thời tìm ra toàn bộ các phản ví dụ vừa tránh việc bộ giải SMT phải giải các tập ràng buộc tương đồng.

CHƯƠNG 2. KIỂM CHỨNG DỰA TRÊN KỸ THUẬT THỰC THI TƯỢNG TRƯNG

2.1. Kỹ thuật thực thi tượng trưng

2.1.1. 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 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

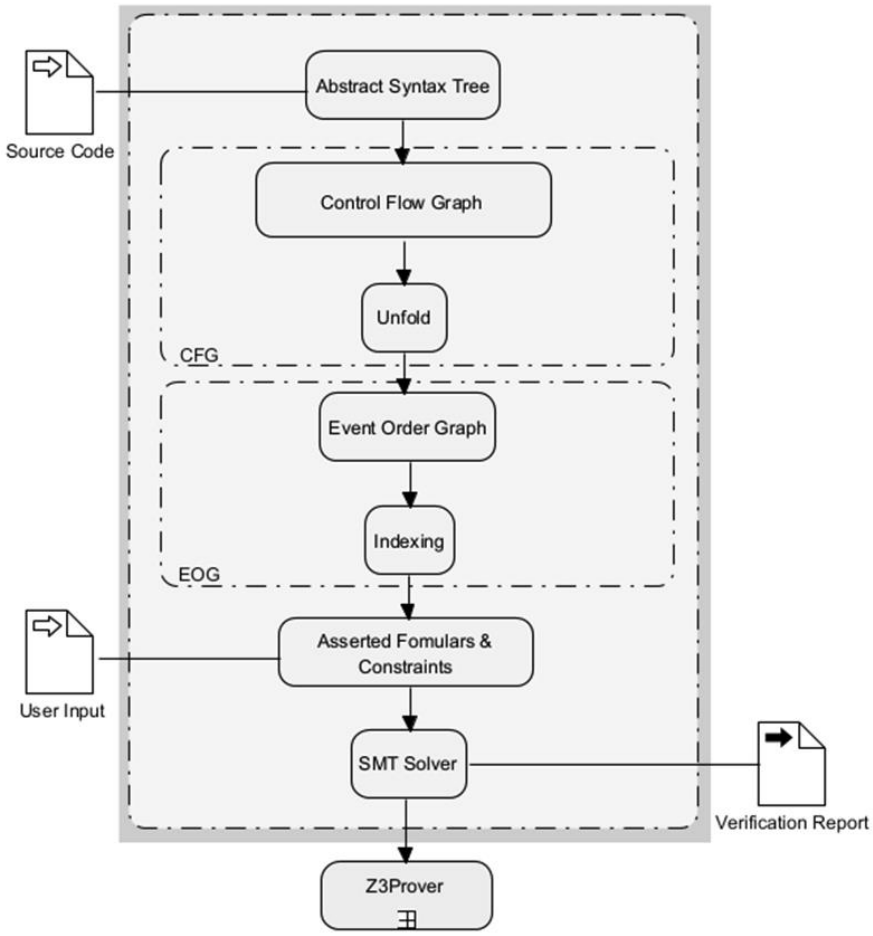
chứng các chương trình lớn vì nó ít bị ảnh hưởng bởi bùng nổ đường thực thi. Tuy nhiên, SSE sẽ gặp phải rất nhiều các vấn đề liên quan đến giá trị động như xử lý vòng lặp và đệ quy do số lượng vòng lặp và số lần đệ quy chỉ được xác định trong trạng thái runtime.

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.

2.1.2. 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 (điều kiện kiểm chứng của người dùng có thể đi kèm luôn trong mã nguồn), 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.

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, nếu mã nguồn không bao gồm điều kiện kiểm chứng, 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.



Hình 2. Kiến trúc thực thi tượng trưng

2.1.3. 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.

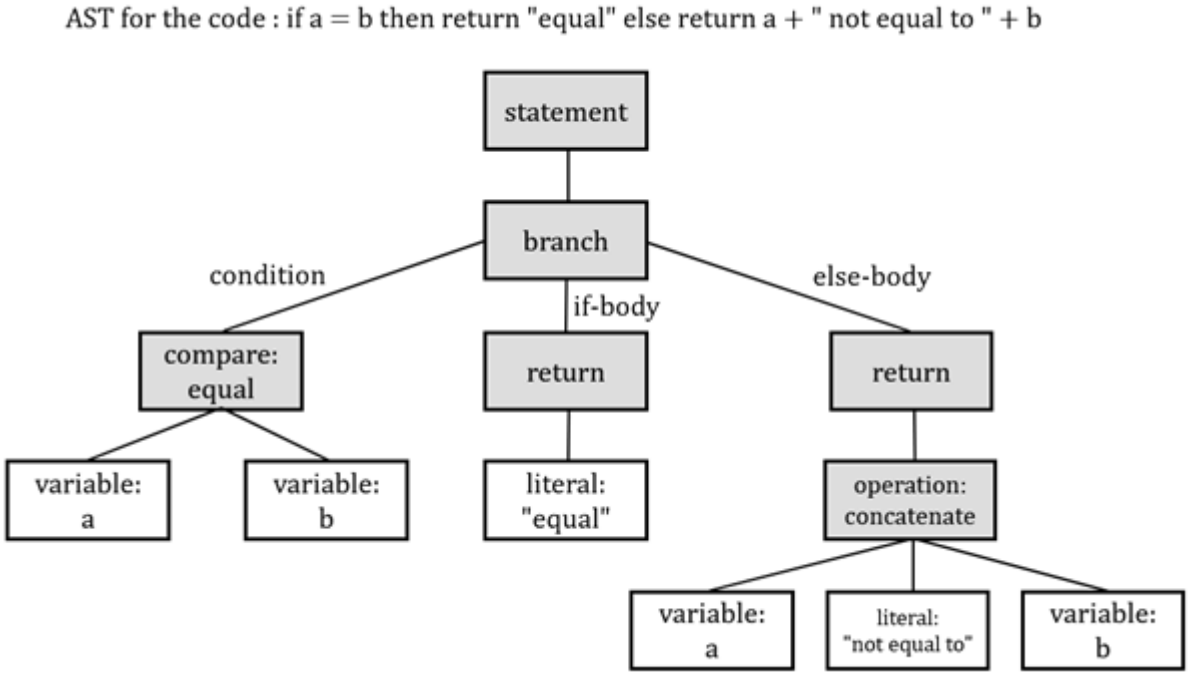
Phần này sẽ trình bày về việc trừu tượng hóa chương trình nhằm mục đích sinh ra cây cú pháp trừu tượng AST và đồ thị luồng điều khiển CFG. Việc xây dựng đồ thị thứ tự sự kiện EOG từ CFG và tổng quát hóa EOG thành các biểu thức logic vị từ cấp một sẽ được trình bày trong các phần sau.

2.1.3.1. 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 3. Abstract Syntax Tree của một khối lệnh đơn giản

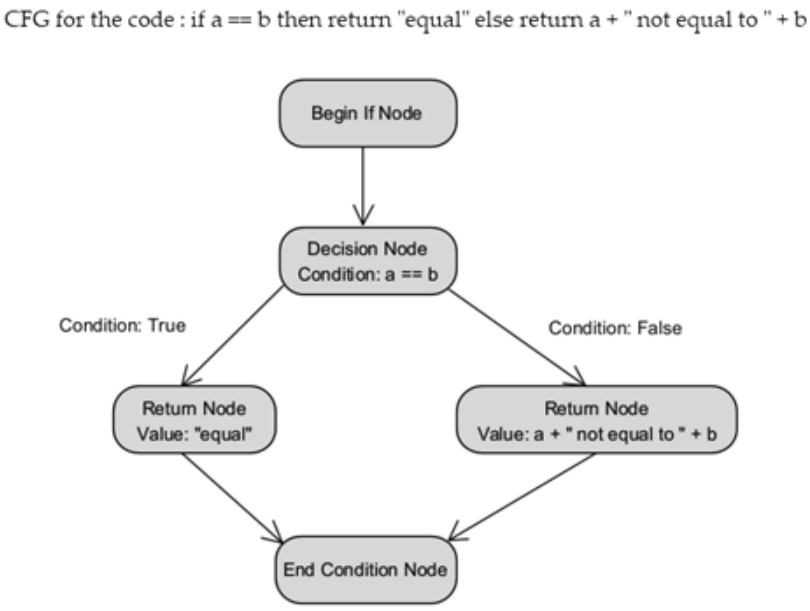
2.1.3.2. Control Flow Graph

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 quan trọng và tạo ra các trường hợp kiểm tra cho tất cả các đường 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 4. Control Flow Graph của một khối lệnh đơn giản

2.2. 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 đồng thời 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.

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

Bộ giải SMT giúp người dùng dễ dàng có thể hình dung được xu hướng lựa chọn luồng thực thi trong quá trình thực hiện chương trình dựa trên việc mô hình hóa các biểu thức điều kiện. Bằng cách thêm vào những điều kiện khác nhau, người dùng có thể sử dụng bộ giải SMT để kiểm tra những nhánh thực thi khác nhau của chương trình, đảm bảo vị trí lưu trữ nào đó luôn có một giá trị cụ thể và thỏa mãn các điều kiện đặt ra.

CHƯƠNG 3. XÂY DỰNG PHƯƠNG PHÁP KIỂM CHỨNG CHƯƠNG TRÌNH ĐA LUỒNG ACIO

3.1. Kiểm chứng dựa trên đồ thị thứ tự sự kiện EOG

Nội dung phần này có tham khảo, sử dụng một phần các định nghĩa và phương pháp của nghiên cứu được trình bày trong tài liệu Scheduling Constraint Based Abstraction Refinement for Multi-Threaded Program Verification [24] *của nhóm tác giả Liangze Yin, Wei Dong, Wanwei Liu và Ji Wang đến từ School of Computer, National University of Defense Technology, China và một số nghiên cứu về kiểm chứng chương trình của các nhóm tác giả khác.*

3.1.1. 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.

*Giả định rằng toàn bộ các biến trong P là nguyên tử, đồng thời toàn bộ các vòng lặp và đệ quy có chiều sâu là giới hạn (điều kiện cơ bản trong Bounded Model Checking, sẽ được trình bày trong mục **3.1.2. 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 $e \in E$ tương ứng với một phần tử biến var(e) $\in V$, 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).

Cho $\prec_P$ là một tập hợp các cặp gồm 2 sự kiện (e_i, e_j) với $e_i \subset E$ và $e_j \subset E$ ($hay \prec_P^0 \subset E \times E$). Mỗi một cặp sự kiện $(e_i, e_j) \in \prec_P$ ($hay\ e_i \prec_P e_j$) biểu thị rằng "sự kiện e_i sẽ xảy ra trước sự kiện ej trong luồng thực thi chương trình P".

Cho $\prec_P^0$ là một tập hợp các cặp gồm 2 sự kiện (e_i, e_j) với $e_i \subset E$ và $e_j \subset E$ ($hay \prec_P^0 \subset E \times E$). Mỗi một cặp sự kiện $(e_i, e_j) \in \prec_P^0$ ($hay\ e_i \prec_P^0 e_j$) biểu thị rằng "sự kiện e_i sẽ xảy ra trước sự kiện e_j trong luồng thực thi chương trình P, dựa trên mã nguồn của P". Nếu $e_i \prec_P^0 e_j$ thì $e_i \prec_P e_j$, hay nói cách khác $\prec_P^0 \subset \prec_P$. Một cặp sự kiện $(e_i, e_j) \in \prec_P^0$ có thể được tạo ra từ các trường hợp sau:

- Với hai sự kiện e_i và e_j trong cùng một luồng, nếu e_i xảy ra trước e_j dựa trên thứ tự câu lệnh trong mã nguồn thì $e_i \prec_P^0 e_j$.
- Nếu *pthread_create()* được dùng để tạo một luồng t tại một điểm p trong luồng hiện tại, với mọi sự kiện e_i xảy ra trước p trong luồng hiện tại và mọi sự kiện e_j trong luồng t thì $e_i \prec_P^0 e_j$.
- 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 e_i trong luồng t và mọi sự kiện e_j xảy ra sau p trong luồng hiện tại thì $e_i \prec_P^0 e_j$.

Cho liên kết đọc-ghi $S(e_i, e_j)$ là một cặp gồm 2 sự kiện e_i và e_j biểu thị rằng "hành động đọc e_j sẽ đọc được giá trị ghi bởi hành động ghi e_i". Điều đó có nghĩa là $e_i \prec_P e_j$, type(e_j) == read, type(e_i) == write, var(e_j) == var(e_i) và value(e_j) == value(e_i). Thêm vào đó, nếu $S(e_i, e_j)$ tồn tại thì với mọi hành động ghi $e_k \neq ei$:

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

Mỗi liên kết đọc-ghi sẽ được biểu diễn tượng trưng bằng một biến boolean 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 trong một luồng thực thi cụ thể thỏa mãn điều kiện đang xét, ngược lại sẽ có giá trị là false.

3.1.2. Bounded Model Checking

Bounded model checking [2] 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/đệ quy có thể được trải phẳng thành các đoạn mã tuyến tính với độ dài giới hạn [7]. Thay vì liệt kê rõ ràng toàn bộ các xen kẽ luồng, BMC sử dụng ký hiệu tượng trưng để thể hiện cho việc mã hóa vấn đề kiểm chứng, thứ sẽ được giải bằng một bộ giải SMT.

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

$$\alpha := \phi_{init} \wedge \rho \wedge \zeta \wedge \xi$$

trong đó, ϕ_{init} 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 $\langle w, r \rangle$, 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" [1].

3.1.3. Đồ thị thứ tự sự kiện EOG

3.1.3.1. Đồ thị thứ tự sự kiện tổng quát

Đồ thị thứ tự sự kiện tổng quát G của một chương trình là biểu diễn đồ thị của kiến trúc trừu tượng α không bao gồm điều kiện khởi đầu và các ràng buộc về liên kết đọc-ghi của chương trình đó:

$$G = graph(\rho) = \langle E, \pounds_n^0 \rangle.$$

với E là tập các đỉnh đọc hoặc ghi tương ứng với các sự kiện đọc hoặc ghi xảy ra trong α và $\pounds_n^0$ là tập các cạnh thể hiện mối quan hệ thứ tự tuyến tính giữa các đỉnh tương ứng với các ràng buộc trong ρ. Mỗi một đỉnh trong G được biểu diễn bằng một nút trắng hoặc đen tương ứng với sự kiện ghi hoặc đọc. Mỗi một cạnh trong G được biểu diễn bằng một đường nối kép đi từ trên xuống dưới.

Việc xây dựng đồ thị thứ tự sự kiện tổng quát G yêu cầu chương trình phải được chuyển về dạng tập hợp các câu lệnh static single assignment (SSA), nghĩa là các biến trong

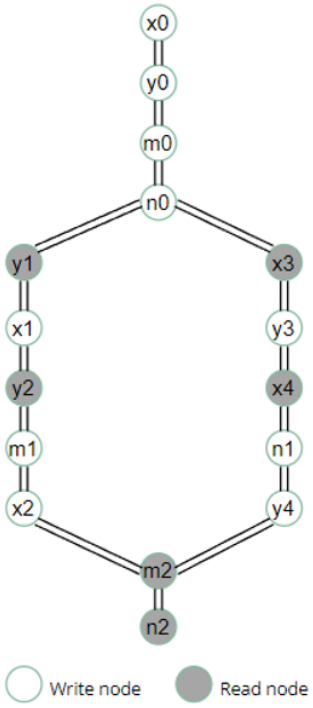
chương trình cần được đổi tên thành các biến đánh dấu giá trị và được sử dụng một lần. Yêu cầu này sẽ đảm bảo mỗi đỉnh và mỗi cạnh được thêm vào trong *G* là duy nhất.

```
int x = 1, y = 1, m = 0, n = 0;
void* thr1(void * arg) {
    x = y + 1;
    m = y;
    x = 0;
}
void* thr2(void * arg) {
    y = x + 1;
    n = x;
    y = 0;
}
void main() {
    pthread_t t1, t2;
    pthread_create(&t1, 0, thr1, 0);
    pthread_create(&t2, 0, thr2, 0);
    pthread_join(t1, 0);
    pthread_join(t2, 0);
    assert (!(m == 2 && n == 3));
}
```

(1) Chương trình gốc

```
int x0 = 1, y0 = 1, m0 = 0, n0 = 0;
void* thr1(void * arg) {
    x1 = y1 + 1;
    m1 = y2 ;
    x2 = 0;
}
void* thr2(void * arg) {
    y3 = x3 + 1;
    n1 = x4 ;
    y4 = 0;
}
void main() {
    pthread_t t1, t2;
    pthread_create(&t1, 0, thr1, 0);
    pthread_create(&t2, 0, thr2, 0);
    pthread_join(t1, 0);
    pthread_join(t2, 0);
    assert (!(m2 == 2 && n2 == 3));
}
```

(2) Mã SSA của chương trình



Hình 5. Xây dựng đồ thị thứ tự sự kiện tổng quát

3.1.3.2. Phản ví dụ

Phản ví dụ π của kiến trúc trừu tượng α tương ứng với điều kiện kiểm chứng ϕ_{verify} là một trình tự thực thi $\pounds_\pi$ của α vi phạm ϕ_{verify}, hay nói cách khác là tập hợp các phép gán giá trị cho các biến trong α thỏa mãn ϕ_{err} với ϕ_{err} là các trạng thái lỗi: $\phi_{err} := \neg \phi_{verify}$. Trình tự thực thi đó được mô tả bằng cách thiết lập một tập các mối quan hệ đọc-ghi giữa các hành động đọc và ghi xảy ra trong α.

$$\pi := \alpha \wedge \pounds_\pi \wedge \phi_{err} \quad \Leftrightarrow \quad \pi := \phi_{init} \wedge \rho \wedge \zeta \wedge \xi \wedge \pounds_\pi \wedge \phi_{err}$$

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

3.1.3.3. Đồ thị thứ tự sự kiện của phản ví dụ

Đồ thị thứ tự sự kiện G_π của phản ví dụ π là sự kết hợp của đồ thị thứ tự sự kiện tổng quát G và biểu diễn đồ thị μ_π của trình tự thực thi $\pounds_\pi$ được mô tả trong π.

$$G_\pi = G \wedge £_\pi = (E, £_n^0, \mu_\pi).$$

G_π được biểu diễn bằng cách biểu diễn đồng thời G *và* $£_\pi$ trên cùng một đồ thị.

μ_π là tập hợp các cạnh thể hiện mối quan hệ đọc-ghi giữa một đỉnh ghi n_1 và một đỉnh đọc n_2 tương ứng đảm bảo rằng $n_1 \prec_P n_2$, var(n_1) = var(n_2), type(n_1) = write, type(n_2) = read, value(n_1) = value(n_2), giữa chúng không có bất kì đỉnh nào ghi đè giá trị và không có bất kì cạnh nào khác được định nghĩa bởi μ_π có đỉnh thứ hai là n_2. Mỗi một cạnh trong μ_π được biểu diễn bằng một đường mũi tên nối từ đỉnh ghi xuống đỉnh đọc.

3.2. Phương pháp biểu diễn ràng buộc

Với đồ thị thứ tự sự kiện $G_\pi = (E, £_n^0, \mu_\pi)$*, các ràng buộc sẽ được xây dựng dựa trên các cạnh của* G_π*, hay nói cách khác là dựa trên các quan hệ tuyến tính* $£_n^0$ *và các liên kết đọc-ghi* μ_π*. Các ràng buộc được chia ra thành 3 nhóm chính:*

- *Ràng buộc độc lập trên các luồng.*
- *Ràng buộc cho các biến đọc/ghi dữ liệu.*
- *Ràng buộc đảm bảo thứ tự thực thi.*

3.2.1. 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 r_i*, thực hiện tính toán trên tập biến này rồi ghi kết quả vào một biến* w_i *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.*

Thuật toán sinh ràng buộc độc lập trên các luồng.

Với mỗi một thao tác ghi sẽ có một phép toán đầu vào đi kèm để xác định giá trị được ghi. Phép toán đầu vào này chứa thao tác đọc giá trị của một số biến nào đó (hoặc có thể không chứa thao tác đọc nếu phép toán chỉ bao gồm các số). Khi biểu diễn thành các đỉnh đọc/ghi trên EOG, mỗi đỉnh ghi trên EOG sẽ có liên hệ với một tập các đỉnh đọc được sử dụng trong phép toán đầu vào tương ứng. Từ mối liên hệ đó, ràng buộc độc lập trên các luồng được sinh ra sử dụng quan hệ ngang bằng giữa giá trị của biến ghi và giá trị của phép toán đầu vào.

Algorithm 1. Independent constraints generation.

Input: EOG $G_\pi := \langle E, £_n^0, \mu_\pi \rangle$.

Output: Set of independent constraints of G_π.

let E_{write} := set of write nodes of G_π.

let $\beta_{independent}$ be initial set of independent constraints.

foreach (write node W in E_{write}) **do**

    let R_s := set of read nodes correspond with W.

    let C_{Rs} := calculation of indexedVar(R_s), corresponding with W.

    $\beta_{independent}$.add(indexedVar(W) = C_{Rs}).

end.

return $\beta_{independent}$.

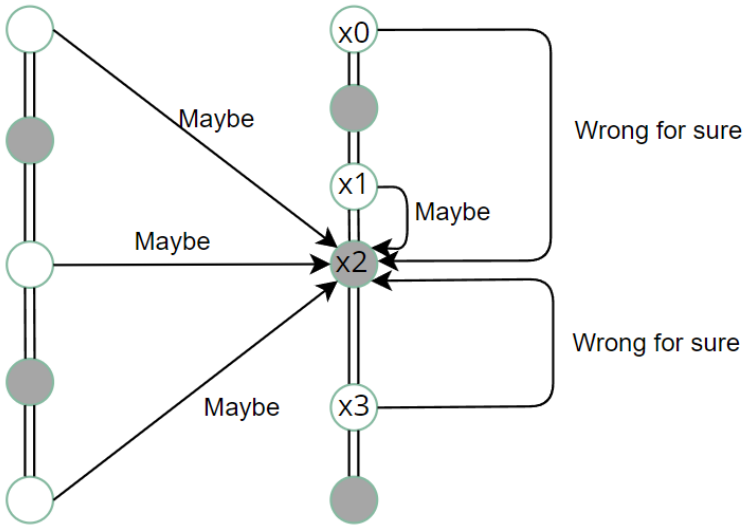
3.2.2. Ràng buộc cho các biến đọc/ghi dữ liệu

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.

Thuật toán sinh ràng buộc cho các biến đọc/ghi dữ liệu.

Với mỗi đỉnh đọc trong EOG sẽ có một tập các đỉnh ghi tương ứng (thao tác lên cùng một biến và có thể xảy ra trước đỉnh đọc). Đỉnh đọc này sẽ liên kết với các đỉnh ghi khả thi để tạo thành các liên kết đọc-ghi $S(e_i, e_j)$. Các liên kết này cần đảm bảo là khả thi. Sau đó, từ tập các liên kết vừa sinh ra, cần đảm bảo rằng trong đó có một và chỉ một liên kết có tồn tại, dựa vào tính chất duy nhất trong mối quan hệ giữa đỉnh đọc và đỉnh ghi trong liên kết đọc-ghi.

Xét ví dụ trong *Hình 6*, đỉnh đọc x_2 cùng thao tác lên một biến với đỉnh ghi x_0, x_1, x_3 và một vài đỉnh trong các luồng khác. Tuy nhiên, khi thực thi hành động đọc x_2 đọc giá trị của biến x thì giá trị x_0 và x_3 đều không tồn tại vì x_1 đã ghi đè giá trị của x_0 và x_3 chưa được thực thi. Điều đó có nghĩa là x_2 không thể liên kết với x_0 hoặc x_3 để tạo thành liên kết đọc ghi. Do đó, $S(x_0, x_2)$ và $S(x_3, x_2)$ là không tồn tại và sẽ không được sử dụng để sinh ràng buộc cho các biến đọc/ghi dữ liệu.



Hình 6. Một số hành động ghi tương ứng với hành động đọc

Algorithm 2. Read/write variables constraints generation.

Input: EOG $G_\pi := \langle E, \pounds_n^0, \mu_\pi \rangle$.

Output: Set of read/write variables constraints of G_π.

let E_{read} := set of read nodes of G_π, let β_{rw} be initial set of read/write variables constraints.

foreach (read node R in E_{read}) **do**

    let W_s := set of write nodes correspond with R and can happen before R.

    let RW_s be initial set of read-write links created by R.

    foreach (write node W in W_s) **do**

        let isValid := true, initial valid status of read-write link between R and W.

        foreach (write node $W_{other} \neq W$ in W_s) **do**

            if ($W \prec_P^0 W_{other}$ and $W_{other} \prec_P^0 R$) **do**

                isValid := false.

                break.

            end.

        end.

        if (!isValid) **do**

            continue.

        end.

        let signature := unique literal defined by R and W.

        let constraint := (signature ⇒ (indexedVar(R) == indexedVar(W)).

        RW_s.add(constraint).

        β_{rw}.add(constraint).

    end.

    let atLeastOne := at least one constraint in RW_s is true.

    let atMostOne := at most one constraint in RW_s is true.

    β_{rw}.add(atLeastOne).

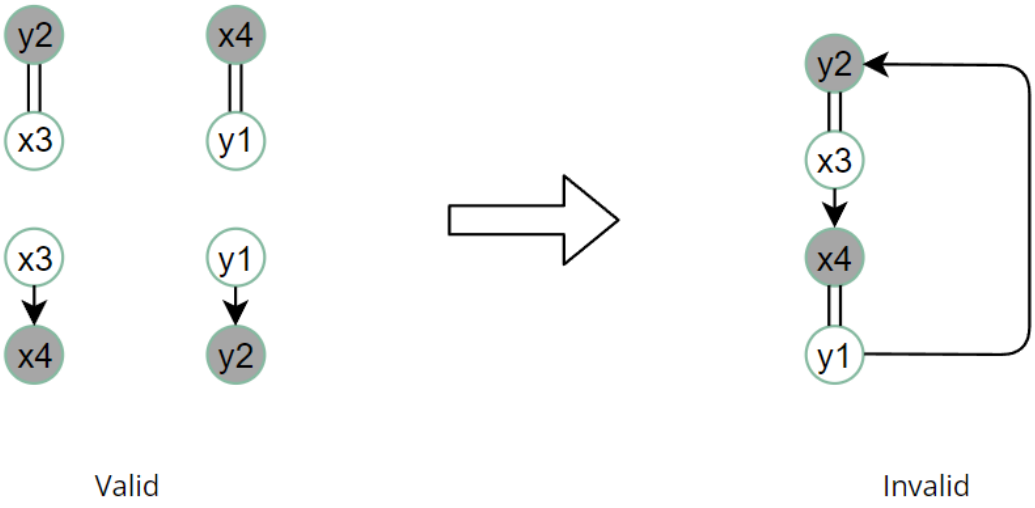
    β_{rw}.add(atMostOne).

end.

return β_{rw}.

3.2.3. Ràng buộc đảm bảo thứ tự thực thi

Có thể thấy rằng ràng buộc cho các biến đọc/ghi dữ liệu chỉ quan tâm đến ràng buộc nội hàm giữa các liên kết đọc-ghi riêng biệt có cùng đỉnh đọc mà không quan tâm đến quan hệ giữa các liên kết đọc-ghi không cùng đỉnh đọc và ràng buộc độc lập trên từng luồng. Bỏ qua các quan hệ đó có thể dẫn tới việc một đỉnh đọc có thể đọc được đỉnh ghi chưa từng xảy ra hoặc đã bị ghi đè bởi đỉnh ghi khác.



Hình 7. Đỉnh đọc đọc được giá trị của một đỉnh ghi chưa xảy ra

Xét ví dụ trong Hình 7, cho rằng hành động Read x_4 có thể đọc được giá trị của hành động Write x_3, hành động Read y_2 có thể đọc được giá trị của hành động Write y_1. Tuy nhiên khi kết hợp với các ràng buộc độc lập trên các luồng vào, hành động Read y_2 lúc này sẽ xảy ra trước hành động Write y_1. Do đó y_1 không thể đọc được giá trị của y_2, liên kết đọc ghi Read y_2 – Write y_1 không tồn tại.

Để khắc phục thiếu sót này, ràng buộc đảm bảo thứ tự thực thi được thêm vào trong quá trình biểu diễn ràng buộc. Ràng buộc đảm bảo thứ tự thực thi phát biểu rằng sự tồn tại của liên kết đọc-ghi này sẽ dẫn đến sự không tồn tại của một số liên kết đọc-ghi khác để đảm bảo rằng các liên kết đọc-ghi không tạo ra xung đột đồng thời thỏa mãn ràng buộc độc lập trên từng luồng.

3.2.3.1. Thuật toán sinh ràng buộc đảm bảo thứ tự thực thi.

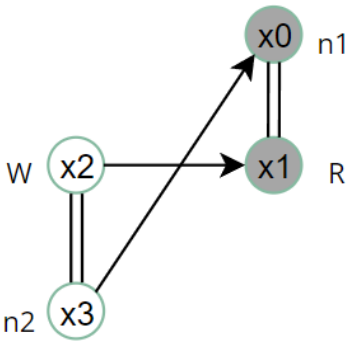
Về tổng quan, ràng buộc này đưa ra các điều kiện để các liên kết đọc-ghi là khả thi trong mối quan hệ với toàn bộ các liên kết đọc ghi khác không cùng đỉnh đọc (có thể hiểu là . Với một liên kết đọc-ghi được tạo ra bởi một đỉnh đọc *R* và một đỉnh ghi *W* cho trước, thuật toán sinh ràng buộc sẽ xem xét 4 nhóm đỉnh được phân thành hai tập hợp:

- Tập hợp 1: gồm các đỉnh xảy ra trước đỉnh đọc *R* và các đỉnh xảy ra sau đỉnh ghi *W*.
- Tập hợp 2: gồm các đỉnh xảy ra sau đỉnh đọc *R* và các đỉnh xảy ra trước đỉnh ghi *W*.

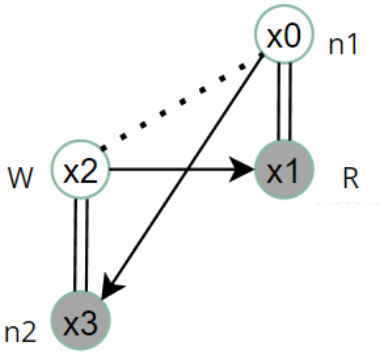
3.2.3.1.1. Thuật toán sinh ràng buộc đảm bảo thứ tự thực thi cho tập hợp 1.

Xét liên kết đọc-ghi được tạo ra bởi từng cặp gồm 2 đỉnh, đỉnh thứ nhất n_1 được chọn trong tập các đỉnh xảy ra trước đỉnh đọc *R* và đỉnh thứ hai n_2 được chọn trong tập các đỉnh xảy ra sau đỉnh ghi *W*.

- Nếu type(n_1) = type(n_2) thì không có xung đột nào do không thể tạo liên kết đọc-ghi giữa hai đỉnh cùng loại.
- Nếu *W* là đỉnh ghi x_2, *R* là đỉnh đọc x_1, n_1 là đỉnh đọc x_0, n_2 là đỉnh ghi x_3, $var(n_1) = var(n_2) = var(R) = var(W) = x$. Khi đó, $R \prec_P W \prec_P^o n_2$. Kết hợp với điều kiện $n1 \prec_P^o R$ sinh ra ràng buộc $n1 \prec_P^o R \prec_P W \prec_P^o n_2$. Lúc này, $S(n_2, n_1)$ là không tồn tại vì n_2 chưa xảy ra khi n_1 được thực thi. (*Hình 8)*
- Nếu *W* là đỉnh ghi x_2, *R* là đỉnh đọc x_1, n_1 là đỉnh ghi x_0, n_2 là đỉnh đọc x_3, $var(n_1) = var(n_2) = var(R) = var(W) = x$. Khi đó, $S(W, R) \rightarrow n_1 \prec_P W \prec_P^o R$. Kết hợp với điều kiện $W \prec_P^o n_2$ sinh ra ràng buộc $n_1 \prec_P W \prec_P^o n_2$. Lúc này, $S(n_1, n_2)$ là không tồn tại do giữa n_1 và n_2 có hành động *W* ghi giá trị vào biến *x*. (*Hình 9)*



Hình 8. Xung đột thứ nhất của tập hợp 1



Hình 9. Xung đột thứ hai của tập hợp 1

Algorithm 3. Execution-order-assurance constraints generation for collection 1.

Input: EOG $G_\pi := \langle E, \pounds_n^0, \mu_\pi \rangle$, read-write link S(W, R).

Output: Set of constraints ensuring execution order of collection 1 of S(W, R) in G_π.

let E_{pR} := set of previous nodes of R.

let E_{aW} := set of following nodes of W.

let $\beta_{guaranteed\_1}$ be initial set of constraints ensuring execution order of collection 1.

foreach (node N_1 in E_{pR}) **do**

    foreach (node N_2 in E_{aW}) **do**

        if (N_1 is instance of read node) **do**

            if (N_2 is instance of write node) **do**

                if (var(N_1) = var(N_2) = var(W) = var(R)) **do**

                    $\beta_{guaranteed\_1}$.add(¬S(N_2, N_1)).

                end.

            end.

        else if (N_1 is instance of write node) **do**

            if (N_2 is instance of read node) **do**

                if (var(N_1) = var(N_2) = var(W) = var(R)) **do**

                    $\beta_{guaranteed\_1}$.add(¬S(N_1, N_2)).

                end.

            end.

        end.

    end.

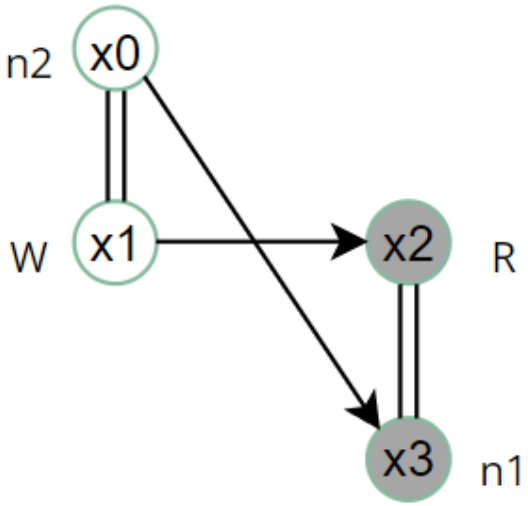
end.

return $\beta_{guaranteed\_1}$.

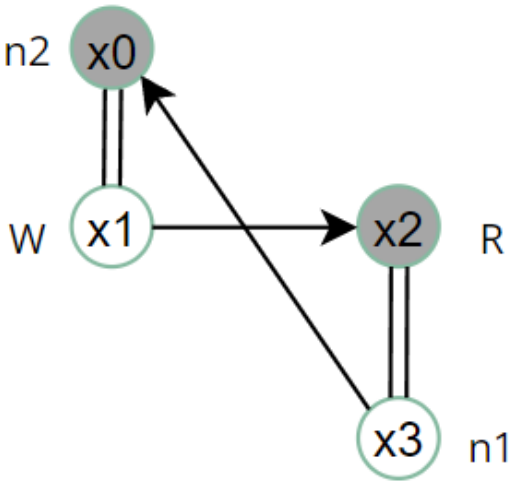
3.2.3.1.2. Thuật toán sinh ràng buộc đảm bảo thứ tự thực thi cho tập hợp 2.

Xét liên kết đọc-ghi được tạo ra bởi từng cặp gồm 2 đỉnh, đỉnh thứ nhất n_1 được chọn trong tập các đỉnh xảy ra sau đỉnh đọc R và đỉnh thứ hai n_2 được chọn trong tập các đỉnh xảy ra trước đỉnh ghi W.

- Nếu type(n_1) = type(n_2) thì không có xung đột nào do không thể tạo liên kết đọc-ghi giữa hai đỉnh cùng loại.
- Nếu W là đỉnh ghi x_1, R là đỉnh đọc x_2, n_1 là đỉnh đọc x_3, n_2 là đỉnh ghi x_0, $var(n_1) = var(n_2) = var(R) = var(W) = x$. Khi đó, từ định nghĩa của liên kết đọc-ghi, $S(W, R) \rightarrow n_2 \prec_P^o W \prec_P R$. Kết hợp với điều kiện $R \prec_P^o n_1$ sinh ra ràng buộc $n_2 \prec_P^o W \prec_P R \prec_P^o n_1$. Lúc này, $S(n_2, n_1)$ là không tồn tại vì giữa n_1 và n_2 có đỉnh W ghi giá trị vào biến x. (*Hình 10*)
- Nếu W là đỉnh ghi x_1, R là đỉnh đọc x_2, n_1 là đỉnh ghi x_3, n_2 là đỉnh đọc x_0, $var(n_1) = var(n_2) = x$. Khi đó, $n_2 \prec_P^o W \prec_P R \prec_P^o n_1$. Lúc này, $S(n_1, n_2)$ là không tồn tại do n_1 chưa xảy ra khi n_2 được thực thi. (*Hình 11*)



Hình 10. Xung đột thứ nhất của tập hợp 2



Hình 11. Xung đột thứ hai của tập hợp 2

Algorithm 4. Execution-order-assurance constraints generation for collection 2.

Input: EOG $G_\pi := \langle E, \pounds_n^0, \mu_\pi \rangle$, read-write link S(W, R).

Output: Set of constraints ensuring execution order of collection 2 of S(W, R) in G_π.

let E_{aR} := set of following nodes of R.

let E_{pW} := set of previous nodes of W.

let $\beta_{guaranteed\_2}$ be initial set of constraints ensuring execution order of collection 2.

foreach (node N_1 in E_{aR}) **do**

  foreach (node N_2 in E_{pW}) **do**

    if (N_1 is instance of read node) **do**

      if (N_2 is instance of write node) **do**

        if (var(N_1) = var(N_2) = var(W) = var(R)) **do**

          $\beta_{guaranteed\_2}$.add(¬S(N_2, N_1)).

        end.

      end.

    else if (N_1 is instance of write node) **do**

      if (N_2 is instance of read node) **do**

        if (var(N_1) = var(N_2)) **do**

          $\beta_{guaranteed\_2}$.add(¬S(N_1, N_2)).

        end.

      end.

    end.

  end.

end.

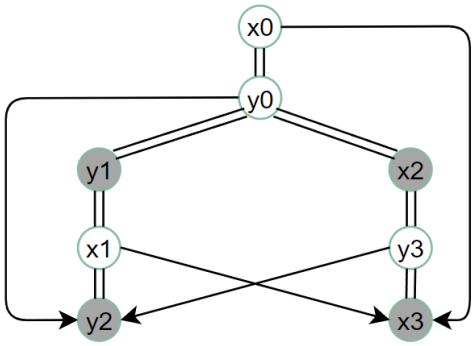
return $\beta_{guaranteed\_2}$.

3.2.3.2. Thuật toán sinh ràng buộc suy diễn đảm bảo thứ tự thực thi.

Xét ví dụ trong *Hình 12*, với liên kết đọc-ghi $S(y_0, y_2)$ và $S(x_0, x_3)$, thuật toán sinh ràng buộc đảm bảo thứ tự thực thi sẽ sinh ra các ràng buộc sau:

$$S(y_0, y_2) \rightarrow \neg S(y_3, y_1)$$

$$S(x_0, x_3) \rightarrow \neg S(x_1, x_2)$$



Hình 12. EOG không được bao phủ hết bằng thuật toán sinh ràng buộc đảm bảo thứ tự thực thi

Có thể thấy rằng, dựa trên thuật toán sinh ràng buộc đảm bảo thứ tự thực thi, hai liên kết này là độc lập, không ràng buộc với nhau. Tuy nhiên, giả sử $S(y_0, y_2)$ có tồn tại, khi đó, $y_0 \prec_P y_2$. y_3 là hành động ghi lên biến y, $y_0 \prec_P^0 y_3$ nên $y_0 \prec_P y_2 \prec_P y_3$ (theo định nghĩa của liên kết đọc-ghi). Lại có $y_3 \prec_P^0 x_3$ nên $y_2 \prec_P y_3 \prec_P^0 x_3$. Dựa vào đồ thị EOG, $x_0 \prec_P^0 x_1 \prec_P^0 y_2$ nên $x_0 \prec_P^0 x_1 \prec_P x_3$. Do x_1 ghi đè lên x_0 trước khi x_3 được thực thi nên $S(x_0, x_3)$ không tồn tại, hay $S(y_0, y_2) \rightarrow \neg\, S(x_0, x_3)$. Điều này chứng minh rằng thuật toán sinh ràng buộc đảm bảo thứ tự thực thi là chưa đầy đủ.

Nguyên nhân là bởi vì điều kiện tiên quyết của thuật toán sinh ràng buộc đảm bảo thứ tự thực thi là sự tồn tại của liên kết đọc-ghi tương ứng. Liên kết đọc-ghi này lại là cơ sở để xác định thứ tự trước sau của các hành động đọc/ghi có quan hệ thứ tự với hai đầu mút của nó. Khi kết hợp với điều kiện ban đầu, một số liên kết đọc-ghi lúc này sẽ trở nên không khả thi. Bởi vậy, thuật toán sinh ràng buộc bổ sung đảm bảo thứ tự thực thi được thêm vào để loại bỏ đi các liên kết đọc-ghi không khả thi mỗi khi một liên kết đọc-ghi được cho rằng là có tồn tại.

Algorithm 5. Deductive constraints ensuring execution order generation.

Input: EOG $G_\pi := \langle E, \pounds_n^0, \mu_\pi \rangle$, read-write link S(W, R).

Output: Set of deductive constraints ensuring execution order of S(W, R) in G_π.

let E_{fWw} := all following write nodes of W that is not in the same thread but has the same var with R .

let E_{pRw} := all previous write nodes of R (sorted by reversed order).

let $\beta_{deductive}$ be initial set of deductive constraints ensuring execution order.

foreach (write node n_1 in E_{fWw}) **do**

    let E_{dr} := all following read nodes of n_1.

    foreach (read node n_2 in E_{dr}) **do**

        let $E_{nearest}$:= the nearest node of R in E_{pRw} that has the same var with n_2.

        foreach (write node n_3 in E_{pRw}) do

            if (n_3 != $E_{nearest}$ and var(n_3) == var(n_2)) **do**

                $\beta_{deductive}$ .add(¬S(n_3, n_2)).

            end.

        end.

    end.

end.

return $\beta_{deductive}$.

Ràng buộc bổ sung đảm bảo thứ tự thực thi phát biểu rằng với mỗi liên kết đọc-ghi *S(w,r)* thao tác lên một biến *v*, *w* thuộc luồng t_1, *r* thuộc luồng t_2, cho n_1 là đỉnh ghi cùng thao tác lên biến *v*, diễn ra sau *w* trong luồng t_1, khi đó toàn bộ các đỉnh đọc r_i xảy ra sau n_1 không thể đọc được giá trị ghi bởi các đỉnh ghi w_i tương ứng nằm trước *r* trong luồng t_2 ngoại trừ $w_{nearest}$ là đỉnh ghi tương ứng gần nhất so với *r*.

Ràng buộc này được chứng minh như sau:

$(S(w, r) \text{ and } w \prec_P^0 n_1) \rightarrow w \prec_P r \prec_P n_1$

$(r \prec_P n_1 \text{ and } n_1 \prec_P^0 r_i) \rightarrow r \prec_P r_i$

Cho $w_1, w_2 \ldots, w_n$ *là đỉnh ghi tương ứng với* r_i *thỏa mãn* $w_1 \prec_P^0 \ldots \prec_P^0 w_n \prec_P^0 r$

$(r \prec_P r_i, w_1 \prec_P^0 \ldots \prec_P^0 w_n \prec_P^0 r) \rightarrow (w_1 \prec_P^0 \ldots \prec_P^0 w_n \prec_P^0 r \prec_P r_i)$

Để hai hành động đọc và ghi tạo thành một liên kết đọc-ghi thì giữa chúng không có bất kì hành động ghi nào, do đó từ suy diễn trên, r_i *không thể tạo được bất kì liên kết đọc ghi nào với* w_i $(0 \leq i \leq n)$ *ngoại trừ* w_n *là đỉnh gần nhất so với r*

3.2.4. Minh họa phương pháp

Lấy chương trình trong Hình 5 làm ví dụ minh họa để xây dựng tập các ràng buộc cho bộ giải SMT. Các bước xây dựng ràng buộc được thực hiện theo trình tự như sau.

3.2.4.1. Xây dựng ràng buộc độc lập trên các luồng

$E_{write} := \{ x_0, y_0, m_0, n_0, x_1, m_1, x_2, y_3, n_1, y_4 \}$

Mỗi đỉnh đọc trong E_{write} có biểu thức tương ứng là:

$x_0 \rightarrow x_0 = 1$ $\quad n_0 \rightarrow n_0 = 0$ $\quad x_2 \rightarrow x_2 = 0$ $\quad n_1 \rightarrow n_1 = x_4$

$y_0 \rightarrow y_0 = 1$ $\quad x_1 \rightarrow x_1 = y_1 + 1$ $\quad y_3 \rightarrow y_3 = x_3 + 1$ $\quad y_4 \rightarrow y_4 = 0$

$m_0 \rightarrow m_0 = 0$ $\quad m_1 \rightarrow m_1 = y_2$

Biểu diễn các biểu thức trên thành ràng buộc tương ứng, thu được ràng buộc độc lập:

$$\beta_{independent} := (x_0 = 1) \wedge (y_0 = 1) \wedge (m_0 = 0) \wedge (n_0 = 0)$$
$$\wedge (x_1 = y_1 + 1) \wedge (m_1 = y_2) \wedge (x_2 = 0)$$
$$\wedge (y_3 = x_3 + 1) \wedge (n_1 = x_4) \wedge (y_4 = 0)$$

3.2.4.2. Xây dựng ràng buộc cho các biến đọc/ghi dữ liệu

E_{read} := { y_1, y_2, x_3, x_4, m_2, n_2 }

Xét lần lượt các sự kiện đọc trong E_{read} thu được các ràng buộc đọc-ghi của từng sự kiện:

- y_1 có thể đọc được giá trị của { y_0, y_3, y_4 }

$$\beta_{rw\_y_1} := (S_{y_0, y_1} \Rightarrow y_1 = y_0) \wedge (S_{y_3, y_1} \Rightarrow y_1 = y_3) \wedge (S_{y_4, y_1} \Rightarrow y_1 = y_4)$$

$$\wedge \text{atLeastOne}(S_{y_0, y_1}, S_{y_3, y_1}, S_{y_4, y_1}) \wedge \text{atMostOne}(S_{y_0, y_1}, E_{y_3, y_1}, S_{y_4, y_1})$$

- y_2 có thể đọc được giá trị của { y_0, y_3, y_4 }

$$\beta_{rw\_y_2} := (S_{y_0, y_2} \Rightarrow y_2 = y_0) \wedge (S_{y_3, y_2} \Rightarrow y_2 = y_3) \wedge (S_{y_4, y_2} \Rightarrow y_2 = y_4)$$

$$\wedge \text{atLeastOne}(S_{y_0, y_2}, S_{y_3, y_2}, S_{y_4, y_2}) \wedge \text{atMostOne}(S_{y_0, y_2}, S_{y_3, y_2}, S_{y_4, y_2})$$

- x_3 có thể đọc được giá trị của { x_0, x_1, x_2 }

$$\beta_{rw\_x_3} := (S_{x_0, x_3} \Rightarrow x_3 = x_0) \wedge (S_{x_1, x_3} \Rightarrow x_3 = x_1) \wedge (S_{x_2, x_3} \Rightarrow x_3 = x_2)$$

$$\wedge \text{atLeastOne}(S_{x_0, x_3}, S_{x_1, x_3}, S_{x_2, x_3}) \wedge \text{atMostOne}(S_{x_0, x_3}, S_{x_1, x_3}, S_{x_2, x_3})$$

- x_4 có thể đọc được giá trị của { x_0, x_1, x_2 }

$$\beta_{rw\_x_4} := (S_{x_0, x_4} \Rightarrow x_4 = x_0) \wedge (S_{x_1, x_4} \Rightarrow x_4 = x_1) \wedge (S_{x_2, x_4} \Rightarrow x_4 = x_2)$$

$$\wedge \text{atLeastOne}(S_{x_0, x_4}, S_{x_1, x_4}, S_{x_2, x_4}) \wedge \text{atMostOne}(S_{x_0, x_4}, S_{x_1, x_4}, S_{x_2, x_4})$$

- m_2 có thể đọc được giá trị của { m_1 }

$$\beta_{rw\_m_2} := (S_{m_1, m_2} \Rightarrow m_2 = m_1) \wedge \text{atLeastOne}(S_{m_1, m_2}) \wedge \text{atMostOne}(S_{m_1, m_2})$$

- n_2 có thể đọc được giá trị của { n_1 }

$$\beta_{rw\_n_2} := (S_{n_1, n_2} \Rightarrow m_2 = m_1) \wedge \text{atLeastOne}(S_{n_1, n_2}) \wedge \text{atMostOne}(S_{n_1, n_2})$$

Kết hợp tất cả ràng buộc đọc-ghi của từng sự kiện thu được ràng buộc cho các biến đọc-ghi của toàn bộ chương trình:

$$\beta_{rw} := \beta_{rw\_y_1} \wedge \beta_{rw\_y_2} \wedge \beta_{rw\_x_3} \wedge \beta_{rw\_x_4} \wedge \beta_{rw\_m_2} \wedge \beta_{rw\_n_2}$$

3.2.4.3. Xây dựng ràng buộc đảm bảo thứ tự thực thi

Những liên kết đọc-ghi không có ràng buộc đảm bảo thực thi sẽ bị bỏ qua và không được đề cập trong phần này.

- Áp dụng Algorithm 3 và 4 lên từng liên kết đọc ghi thu được:

$$\beta_{guaranteed} := \beta_{guaranteed\_1} \wedge \beta_{guaranteed\_2} = (S_{x_1, x_4} \Rightarrow \neg S_{x_2, x_3} \text{ and } \neg S_{y_4, y_1})$$
$$\wedge (S_{x_0, x_4} \Rightarrow \neg S_{x_1, x_3} \text{ and } \neg S_{x_2, x_3})$$
$$\wedge (S_{x_2, x_4} \Rightarrow \neg S_{y_4, y_2} \text{ and } \neg S_{y_4, y_1})$$
$$\wedge (S_{x_1, x_3} \Rightarrow \neg S_{y_3, y_1} \text{ and } \neg S_{x_0, x_4} \text{ and } \neg S_{y_4, y_1})$$
$$\wedge (S_{x_2, x_3} \Rightarrow \neg S_{y_3, y_2} \text{ and } \neg S_{y_3, y_1} \text{ and } \neg S_{x_1, x_4}$$
$$\text{and } \neg S_{x_0, x_4} \text{ and } \neg S_{y_4, y_2} \text{ and} \neg S_{y_4, y_1})$$
$$\wedge (S_{y_0, y_2} \Rightarrow \neg S_{y_3, y_1} \text{ and } \neg S_{y_4, y_1})$$
$$\wedge (S_{y_4, y_2} \Rightarrow \neg S_{x_2, x_4} \text{ and } \neg S_{x_2, x_3})$$
$$\wedge (S_{y_3, y_2} \Rightarrow \neg S_{y_4, y_1} \text{ and } \neg S_{x_2, x_3})$$
$$\wedge (S_{y_3, y_1} \Rightarrow \neg S_{x_1, x_3} \text{ and } \neg S_{y_0, y_2} \text{ and } \neg S_{x_2, x_3})$$
$$\wedge (S_{y_4, y_1} \Rightarrow \neg S_{x_1, x_4} \text{and } \neg S_{x_1, x_3} \text{and } \neg S_{y_3, y_2}$$
$$\text{and } \neg S_{y_0, y_2} \text{ and } \neg S_{x_2, x_4} \text{ and} \neg S_{x_2, x_3})$$

- Áp dụng Algorithm 5 vào từng liên kết đọc-ghi thu được:

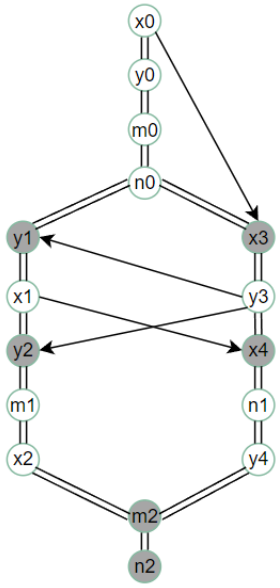
$$\beta_{deductive} := (S_{x_0, x_4} \Rightarrow \neg S_{y_0, y_2}) \wedge (S_{y_0, y_2} \Rightarrow \neg S_{x_0, x_4})$$

3.2.4.4. Kết quả kiểm chứng

Với điều kiện kiểm chứng ϕ_{verify} = !(*m* == 2 && *n* == 3), ϕ_{error} = (*m* == 2 && *n* == 3), bộ giải SMT z3Prover đưa ra kết quả SATISFIABLE cho phản ví dụ $\pi := \phi_{init} \wedge \rho \wedge \zeta \wedge \xi \wedge \pounds_{\pi} \wedge \phi_{err}$ với ρ:= $\beta_{independent}$, $\zeta := \beta_{rw}$ và $\xi := \beta_{guaranteed} \wedge \beta_{deductive}$. Các liên kết đọc ghi được cho là tồn tại trong π là { $S_{x_0, x_3}, S_{y_3, y_1}, S_{x_1, x_4}, S_{y_3, y_2}$ }

Phản ví dụ π biểu diễn cho trình tự thực thi sau:

```
x = 1;                  // x = 1
y = 1;                  // y = 1
m = 0;                  // m = 0
n = 0;                  // n = 0
y = x +1;               // y = 2
x = y + 1;              // x = 3
m = y || n = x;         // m = 2 || n = 3
x = 0 || y = 0;         // x = 0 || y = 0
assert(!(m == 2 && n == 3));        // false
```



Hình 13. EOG của phản ví dụ π

CHƯƠNG 4. THỰC NGHIỆM & ĐÁNH GIÁ

4.1. Thực nghiệm

4.1.1. Tiêu chuẩn của SV-COMP 2017

Các tiêu chuẩn của Competition on Software Verification (SV-COMP) được tạo ra với mục tiêu so sánh các kỹ thuật và công cụ đã được chấp nhận rộng rãi để xác minh chương trình. Một số lượng đáng kể các nghiên cứu về xác minh chương trình đa luồng đã thực hiện các thử nghiệm của họ trên chúng.

Tiêu chuẩn của SV-COMP 2017 về kiểm chứng chương trình đa luồng có 1047 ví dụ là các chương trình đa luồng được viết trên ngôn ngữ C. Tuy nhiên, do giới hạn về thời gian và chi phí, khóa luận này sẽ chỉ thực nghiệm 18 ví dụ trong số 1047 ví dụ kể trên.

1. nondet-loop-bound-1.c [11]
2. nondet-loop-bound-2.c [12]
3. read_write_lock-1.c [13]
4. read_write_lock-1b.c [14]
5. read_write_lock-2.c [15]
6. stateful01-1.c [16]
7. stateful01-2.c [17]
8. triangular-1.c [18]
9. triangular-2.c [19]
10. triangular-longer-1.c [20]
11. triangular-longer-2.c [21]
12. triangular-longest-1.c [22]
13. triangular-longest-2.c [23]
14. peterson-b.c [8]
15. reorder_c11_bad-10.c [3]
16. reorder_c11_bad-30.c [4]
17. reorder_c11_good-10.c [5]
18. reorder_c11_good-10.c [6]

4.1.2. Điều kiện thực nghiệm

Toàn bộ 18 ví dụ sẽ được chạy thực nghiệm trên máy tính sử dụng CPU AMD Ryzen 5 4600H 3GHz 8GB RAM với thời gian giới hạn trong 900000ms (900s). Nếu vượt quá thời gian giới hạn, công cụ sẽ ngừng kiểm chứng ví dụ hiện tại và trả về kết quả NOTSURE.

4.1.3. Kết quả thực nghiệm

Kết quả thực nghiệm của công cụ ACIO với tập các chương trình thực nghiệm được trình bày trong Bảng 1 với các tham số báo cáo là số vòng lặp được giới hạn, số lượng ràng buộc được sinh ra, thời gian sinh và giải các ràng buộc kèm theo đó là kết quả của bộ giải SMT Z3Prover. Kết luận cuối cùng được suy ra từ kết quả của bộ giải SMT và thời gian bộ giải SMT giải các ràng buộc như sau:

- SATISFIABLE & Not timeout ⇒ Vi phạm điều kiện kiểm chứng, NOT SAFE
- UNSATISFIABLE & Not timeout ⇒ Không vi phạm điều kiện kiểm chứng, SAFE
- UNSATISFIABLE & Timeout ⇒ Không chắc chắn kết quả, NOT SURE

Bảng 1. Kết quả thực nghiệm của phương pháp ACIO

Chương trình	Số vòng lặp được giới hạn (nếu có)	Kết quả của bộ giải SMT	Số lượng ràng buộc	Thời gian sinh ràng buộc (ms)	Thời gian giải ràng buộc (ms)	Kết luận
nondet-loop-bound-1.c	20	SAT	950	29	3290	NOT SAFE
nondet-loop-bound-2.c	20	UNSAT	950	23	Timeout	NOT SURE
read_write_lock-1b.c		UNSAT	156	40	20	SAFE
read_write_lock-1.c		UNSAT	172	18	17	SAFE
read_write_lock-2.c		UNSAT	180	17	14	SAFE
stateful01-1.c		SAT	40	9	12	NOT SAFE
stateful01-2.c		SAT	40	8	10	NOT SAFE
triangular-1.c	5	UNSAT	207	13	86	SAFE
triangular-2.c	5	SAT	207	13	27	NOT SAFE
triangular-longer-1.c	10	UNSAT	697	80	140248	SAFE
triangular-longer-2.c	10	SAT	697	84	9543	NOT SAFE
triangular-longest-1.c	20	UNSAT	2577	1313	Timeout	NOT SURE
triangular-longest-2.c	20	UNSAT	2577	1332	Timeout	NOT SURE
peterson-b.c		UNSAT	52	72	34	SAFE
reorder_c11_bad-10.c	10	SAT	98	15	15	NOT SAFE
reorder_c11_bad-30.c	30	SAT	258	17	21	NOT SAFE
reorder_c11_good-10.c	10	UNSAT	98	19	9	SAFE
reorder_c11_good-30.c	30	UNSAT	258	15	9	SAFE

4.2. Đánh giá thực nghiệm

Từ kết quả được trình bày trong *Bảng 1*, có thể thấy rằng phương pháp ACIO đặc biệt hiệu quả với các chương trình nhỏ và vừa với số lượng ràng buộc sinh ra không quá lớn. Bằng phương pháp mã hóa một lần, công cụ ACIO đã giải đúng được bài toán kiểm thử trên 15/18 chương trình với thời gian tiêu hao ít nhất (bao gồm cả sinh và giải ràng buộc) là 18ms trên chương trình *stateful-01-2.c*.

Tuy nhiên, công cụ ACIO cho hiệu quả không cao trên những chương trình phức tạp có số vòng lặp giới hạn kèm theo số lượng ràng buộc lớn, đặc biệt là những chương trình không vi phạm điều kiện kiểm chứng. Việc mã hóa và giải một số lượng lớn các ràng buộc cùng một lúc trực tiếp đặt gánh nặng lên bộ giải mã SMT, dẫn đến việc bùng nổ thời gian, đặc biệt là với các tập hợp ràng buộc cho kết quả UNSAT. Ví dụ điển hình cho sự kém hiệu quả này là kết quả kiểm chứng của hai chương trình *triangular-longer-1.c* và *triangular-longer-2.c*. *triangular-longer-2.c* với kết quả SAT - NOT SAFE chỉ mất 9534ms (9,5s) để giải các ràng buộc, trong khi *triangular-longer-1.c* với kết quả UNSAT - SAFE cần đến 140248ms (140,2s), dù rằng mã nguồn và thời gian sinh ràng buộc của hai chương trình là tương đương, chỉ khác nhau ở điều kiện kiểm chứng. Ngoài ra có thể kể đến chương trình *triangular-longest-1.c* và *triangular-longest-2.c* bị timeout và cho kết quả NOT SURE với 2577 ràng buộc được sinh ra. Tuy nhiên, trong kiểm chứng phần mềm, việc đưa ra kết quả NOT SURE không gây hậu quả quá nghiêm trọng như việc đưa ra kết quả SAFE khi chương trình có lỗi nên kết quả này có thể chấp nhận được.

KẾT LUẬN

Khóa luận đã tìm hiểu và trình bày phương pháp mã hóa chương trình bằng cách sử dụng Đồ thị thứ tự sự kiện EOG cũng như cách thức kết hợp EOG với thực thi tượng trưng để kiểm chứng chương trình đa luồng được viết trên ngôn ngữ C/C++. Đồng thời, công cụ kiểm chứng ACIO cũng được phát triển để chứng minh tính khả thi của phương pháp. Công cụ ACIO bao gồm các thành phần trừu tượng hóa như Cây cú pháp trừu tượng AST, Đồ thị luồng điều khiển CFG tích hợp với EOG để sinh các ràng buộc đọc-ghi.

Với bộ thực nghiệm của SV-COMP 2017, ACIO cho kết quả rất khả quan trên những chương trình nhỏ và vừa với thời gian tiêu hao chỉ tính bằng millisecond.

Trong tương lai, để cải thiện kết quả của ACIO thì bổ sung thêm các điều kiện hoặc chiến thuật duyệt đồ thị EOG để sinh ràng buộc là rất quan trọng. Tăng hiệu quả trong việc duyệt EOG có thể làm giảm thiểu đi các ràng buộc và liên kết đọc-ghi dư thừa, giúp giảm gánh nặng lên bộ giải SMT. Đồng thời, ACIO có thể mở rộng khả năng ứng dụng bằng cách bổ sung thêm các tính chất khác của mã nguồn C/C++ như các kiểu dữ liệu phức tạp (mảng, con trỏ, chuỗi...) và các cấu trúc phức tạp (struct, các lệnh rẽ nhánh, các vòng lặp...).

TÀI LIỆU THAM KHẢO

[1] 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.

[2] 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.

[3] Hongyu Fan, “SV_COMP 2017 Benchmark reorder_c11_bad-10.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread-deagle/reorder_c11_bad-10.c.

[4] Hongyu Fan, “SV_COMP 2017 Benchmark reorder_c11_bad-30.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread-deagle/reorder_c11_bad-30.c.

[5] Hongyu Fan, “SV_COMP 2017 Benchmark reorder_c11_good-10.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread-deagle/reorder_c11_good-10.c.

[6] Hongyu Fan, “SV_COMP 2017 Benchmark reorder_c11_good-30.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread-deagle/reorder_c11_good-30.c.

[7] Shaz Qadeer, Jakob Rehof, "Context-Bounded Model Checking of Concurrent Software," in *International Conference on Tools and Algorithms for Construction and Analysis of Systems*, 2005, pp. 93-107.

[8] Hernan Ponce de Leon , "SV_COMP 2017 Benchmark peterson-b.c," [Online]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread-atomic/peterson-b.c.

[9] L.-M.-U. München, “SV-COMP - International Competition on Software Verification,” Ludwig-Maximilians-Universität München, [Trực tuyến]. Available: https://sv-comp.sosy-lab.org/.

[10] 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/.

[11] Philipp Wendler, "SV_COMP 2017 Benchmark nondet-loop-bound-1.c," [Online]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread-nondet/nondet-loop-bound-1.c.

[12] Philipp Wendler, “SV_COMP 2017 Benchmark nondet-loop-bound-2.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread-nondet/nondet-loop-bound-2.c.

[13] Philipp Wendler, “SV_COMP 2017 Benchmark read_write_lock-1.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread-atomic/read_write_lock-1.c.

[14] Philipp Wendler, “SV_COMP 2017 Benchmark read_write_lock-1b.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread-atomic/read_write_lock-1b.c.

[15] Philipp Wendler, “SV_COMP 2017 Benchmark read_write_lock-2.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread-atomic/read_write_lock-2.c.

[16] Philipp Wendler, “SV_COMP 2017 Benchmark stateful01-1.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread/stateful01-1.c.

[17] Philipp Wendler, “SV_COMP 2017 Benchmark stateful01-2.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread/stateful01-2.c.

[18] Philipp Wendler, “SV_COMP 2017 Benchmark triangular-1.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread/triangular-1.c.

[19] Philipp Wendler, “SV_COMP 2017 Benchmark triangular-2.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread/triangular-2.c.

[20] Philipp Wendler, “SV_COMP 2017 Benchmark triangular-longer-1.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread/triangular-longer-1.c.

[21] Philipp Wendler, “SV_COMP 2017 Benchmark triangular-longer-2.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread/triangular-longer-2.c.

[22] Philipp Wendler, “SV_COMP 2017 Benchmark triangular-longest-1.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread/triangular-longest-1.c.

[23] Philipp Wendler, “SV_COMP 2017 Benchmark triangular-longest-2.c,” [Trực tuyến]. Available: https://gitlab.com/sosy-lab/benchmarking/sv-benchmarks/-/blob/main/c/pthread/triangular-longest-2.c.

[24] 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.