**Automatic test data generation for path testing**

**using adjustment**

**1. Tóm tắt nội dung bài báo**

**2. Tổng quan**

+ Kiểm thử phần mềm và sinh dữ liệu kiểm thử phần mềm

Kiểm thử phần mềm là quá trình thực hiện một chương trình hoặc ứng dụng nào đó với mục đích là tìm kiếm các lỗi phần mềm. Nó cũng có thể được coi như là một quá trình xác nhận và chứng minh rằng một chương trình phần mềm, ứng dụng hoặc sản phẩm đáp ứng đầy đủ các yêu cầu nghiệp vụ và kỹ thuật của thiết kế và phát triển. Kiểm thử phần mềm là một phần rất quan trọng nhưng tốn nhiều công sức trong chu trình phát triển phần mềm [1–3]. Do đó đã có nhiều nghiên cứu về kiểm thử tự động, để giảm chi phí và đạt được sự tin tưởng hơn trong kết quả thu được [4].

Công việc quan trọng trong kiểm thử phần mềm là tạo ra input dữ liệu kiểm thử [3]. Search-based test data generation mục đích là để tự động hóa công việc này, bằng cách tìm kiếm các test case (là các input data, hoặc là cả input-output) mà thỏa mãn một tiêu chuẩn kiểm thử đã được lựa chọn.

+ Phương pháp kiểm thử phần mềm sử dụng các kỹ thuật metaheuristic (Search Based Software Testing)

+ Phương pháp sinh dữ liệu kiểm thử phần mềm sử dụng metaheuristic

+ Khái niệm CFG

+ Khái niệm xác suất phủ của đường dẫn trong chương trình

**3. Bài toán sinh dữ liệu kiểm thử đường dẫn**

+ Bài toán sinh dữ liệu kiểm thử đường dẫn

Kiểm thử đường dẫn là tìm kiếm trong toàn bộ chương trình các test case phù hợp để có thể phủ được toàn bộ các đường dẫn khả thi trong chương trình được thực hiện kiểm thử (software under test (SUT)). Tuy nhiên nhìn chung là không thể thực hiện được mục tiêu này vì một số lý do. Đầu tiên là chương trình có thể có một số lượng vô hạn các đường dẫn nếu trong chương trình có các vòng lặp. Thứ hai, số lượng đường dẫn trong một chương trình là hàm mũ của số lượng các câu lệnh rẽ nhánh và nhiều đường dẫn trong số đó là không thể thực thi được. Thứ ba, số lượng test case sẽ là rất lớn vì mỗi đường dẫn có thể được phủ được bởi nhiều test case. Vì những lý do này, để có thể tạo dữ liệu kiểm thử mà phủ được toàn bộ các đường dẫn của chương trình thì bài toán sinh dữ liệu kiểm thử đường dẫn trở thành bài toán NP-đầy đủ.

Vì không thể phủ toàn bộ các đường dẫn trong một chương trình, thế nên bài toán sinh dữ liệu kiểm thử đường dẫn sẽ chọn ra một tập các đường dẫn để thực thi và tìm các dữ liệu kiểm thử để phủ được chúng. Có nhiều phương pháp sinh dữ liệu kiểm thử đã được đề xuất cho đến thời điểm hiện tại, và có thể được phân chia như là: sinh dữ liệu kiểm thử ngẫu nhiên, symbolic execution hay là các phương pháp tối thiểu hóa hàm. Sinh data ngẫu nhiên là lựa chọn các dữ liệu kiểm thử ngẫu nhiên từ tập các biến input. Symbolic execution là phương pháp phân tích chương trình tĩnh, từ mỗi đường dẫn của chương trình sẽ có được một tập các biểu thức logic biểu diễn cho các điều kiện vị từ của đường dẫn đó, rồi sau đó dùng các constraint solver để tìm được nghiệm cho các biểu thức logic, cũng chính là dữ liệu kiểm thử để phủ đường dẫn này [cần dẫn chứng paper về JPF]. Các phương pháp tối thiểu hóa hàm, hãy cách gọi khác khác phân tích động, vì chúng dựa trên sự thực thi của chương trình. Chúng sẽ thực hiện tìm kiếm thăm dò mà trong đó các biến input được chọn sẽ được thay đổi giá trị một chút rồi chuyển lại cho chương trình cần kiểm thử [cần dẫn chứng paper của Korel].

+ Giả thuyết về hạn chế của phương pháp sinh dữ liệu kiểm thử đường dẫn sử dụng giải thuật di truyền. Giả thuyết này sẽ được kiểm chứng bằng thực nghiệm.

Trong bài báo này, giải thuật di truyền (genetic algorithm - GA) được sử dụng như là một bộ sinh dữ liệu kiểm thử. Mỗi nhiễm sắc thể biểu diễn một tập của dữ liệu kiểm thử (là một tập các giá trị input mà đại diện cho một test case đơn lẻ). Do đó một quần thể là một tập của các test case. Mỗi test case sẽ xác định được một đường dẫn thực thi nó, và phần lớn thì một đường dẫn có thể được phủ bởi nhiều test case. Điều này dẫn đến là một tập các test case có thể dẫn đến toàn bộ các đường dẫn sẽ được phủ.

Các bước cơ bản của GA là (1) Initialization, (2) Evaluation, and (3) Do the following until any stopping criteria is met: (3.a) Selection, (3.b) Perturbation, and (3.c) Go back to Step (2). Ở bước (1) khi sinh quần thể đầu tiên, thì có thể khởi tạo ngẫu nhiên hoặc là sử dụng một số tri thức về quần thể đó. Bước (2) sẽ đánh giá toàn bộ cá thể của quần thể sử dụng một hàm mục tiêu cho trước. Trong (3.a) thì có một số cá thể trong quần thể được lựa chọn để đột biến bằng các xử lý tiến hóa. Bước (3.b) sẽ áp dụng các xử lý: trao đổi chéo để trộn lẫn các gen di truyền và đột biến để giới thiệu các đặc điểm di truyền mới. Bộ sinh test data giữ một danh sách của các đường dẫn mục tiêu mà chưa được phủ. Tại thời điểm bắt đầu sự tiến hóa, mọi đường dẫn mục tiêu đều nằm trong danh sách này. Ở mỗi thế hệ, mỗi dữ liệu kiểm thử trong quần thể được đánh giá (hàm mục tiêu của nó được gọi) để hướng đến các đường dẫn chưa được phủ. Khi một dữ liệu kiểm thử phủ được một đường dẫn mục tiêu, nó được ghi lại và đường dẫn mục tiêu này được loại ra khỏi danh sách. Quá trình tìm kiếm sẽ kết thúc nếu danh sách các đường dẫn mục tiêu là rỗng, hoặc là gặp phải tiêu chuẩn dừng tìm kiếm.

Tuy nhiên trong thực tế giải thuật di truyền khi áp dụng vào bài toán sinh dữ liệu kiểm thử đường dẫn là rất khó để sinh ra dữ liệu kiểm thử của các đường dẫn có xác suất thấp được phủ thấp trong chương trình. Bây giờ chúng ta xét đến bài toán phân loại tam giác Tritype như sau:

int Tritype(double a, double b, double c)

{

int trityp = 0;

if ((a + b > c) && (b + c > a) && (c + a > b))

{

if ((a != b) && (b != c) && (c != a))

trityp = 1; // Scalene

else

if (((a == b) && (b != c)) || ((b == c) && (c != a)) ||

((c == a) && (a != b)))

trityp = 2; // Isosceles

else

trityp = 3; // Equilateral

}

else

trityp = -1; // Not a triangle

return trityp;

}

CFG được sinh ra từ chương trình phân loại tam giác này như sau:



Tập target paths của được sinh ra từ CFG của chương trình phân loại tam giác sẽ có 4 path như sau:

{[B1,False]} // Not Triangle

{[B1,True], [B2,True]} // Scalence

{[B1,True], [B2,False] , [B3,True]} // Isosceles

{[B1,True], [B2,False] , [B3,False]} // Equilateral

+ Giả thuyết về hiệu quả của việc kết hợp giải thuật di truyền (GA) với phân tích tĩnh. Giả thuyết này cũng sẽ được kiểm chứng bằng thực nghiệm.

**4. Thiết kế các giải thuật**

GA và GA + Static Analysis cho bài toán sinh dữ liệu kiểm thử đường dẫn.

**5. Thí nghiệm và phân tích kết quả**

+ Các test programs + target paths

+ Các thông số cần phân tích: Em cần chạy mỗi test program với 2 giải thuật: GA (Không điều chỉnh), GA+ static Analysis (có điều chỉnh). Chạy 30 lần cho mỗi cặp giải thuật + test program. Ghi lại số thế hệ và lần gọi objective function của một đường dẫn mục tiêu khi nó được thực thi.

+ Phân tích kết quả: Phân tích chỉ ra GA không có khả năng phủ được các đường dẫn khó (có điều kiện bằng), trong khi GA + Static Analysis có thể. So sánh 2 giải thuật về số lượng đường dẫn trung bình phủ được trong 30 lần với mỗi test program. Phân tích chi tiết về các đường dẫn phủ được và không phủ được của cả 2 phương pháp, và thời điểm mà chúng được phủ...

**6. Kết luận và hướng phát triển**

**7. Tài liệu tham khảo**

[1] J.A. Whittaker, What is software testing? and why is it so hard?, IEEE Software 17 (1), 02/2000, 70–79.

[2] N. Mansour, M. Salame, Data generation for path testing, Software Quality Control 12(2), 06/2004, 121–136.

[3] P. McMinn, Search-based software test data generation: a survey, Software Testing, Verification & Reliability14 (2), 06/2004, 105–156.

[4] P.M.S. Bueno, M. Jino, Identification of potentially infeasible program paths by　monitoring the search for test data, Proceedings of the 15th IEEE　International Conference on Automated Software Engineering 2000 (ASE2000), IEEE Computer Society, Grenoble, France, 09/2000, 209–218.

[x] I. Hermadi, C. Lokan, R. Sarker, Dynamic stopping criteria for search-based test data generation for path testing, Information and Software Technology, 56 (4), 04/2014,395–407.