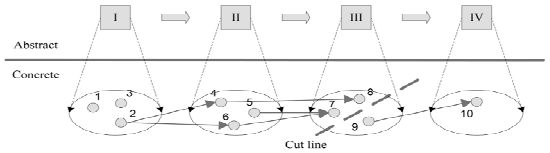


Hình 1: Hệ thống trừu tượng [7]

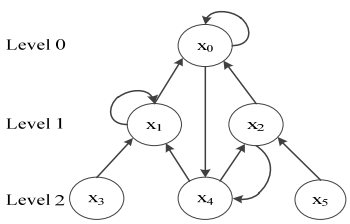
2.1.2 Giải thuật đa trừu tượng

Qian K. *et al.*[13] đề xuất chiến thuật *đa trừu tượng* để giảm chi phí kiểm tra. Dựa trên giả thuyết có các chuỗi mô hình trừu tượng $M_0 \subseteq M_1 \subseteq \ldots$ sao cho trạng thái trừu tượng S^i trên mô hình M_i được tách ra nhiều trạng thái S^{i1}, S^{i2},… trên M_{i+1} (mức độ trừu tượng của M_i nhiều hơn M_{i+1},). Giải thuật tìm kiếm chạy qua các mô hình trừu tượng theo thứ tựM_0, M_1,…tìm kiếm các vi phạm trong các mô hình trừu tượng này. Quá trình tìm kiếm có thể dừng lại nếu không tìm thấy bất kỳ counter-example nào trong bất cứ M_i. Ngược lại, quá trình tìm kiếm tiếp tục phát hiện ra lỗi trên các mô hình trừu tượng còn lại thậm chí là trên mô hình gốc. Giải thuật đa trừu tượng đối xử với tất cả các mô hình trừu tượng như các mô hình riêng rẽ và theo thứ tự. Nó chỉ xem thông tin có được về counter-example của mô hình trừu tượng trong lần tìm kiếm trước đó là heuristic. Dĩ nhiên, vấn đề các trạng thái trừu tượng có kết nối với nhau nhưng thật sự trên mô hình thật các trạng thái không có đường nối giữa chúng (non-strong connected abstract state) vẫn còn tồn tại khi kết quả có thể dẫn tới lần tìm kiếm kế tiếp bị sai đường. Trong trường hợp xấu nhất, giải thuật phải thực thi trên mô hình thật để tìm ra counter-example thật sự.

Tuy hiệu suất của giải thuật đa trừu tượng [13] rất tốt, nó vẫn cần được cải thiện để sử dụng lại thông tin từ giai đoạn tìm kiếm trước đó để chỉ tập trung vào các vùng đáng nghi ngờ trong mô hình trừu tượng kế tiếp có khả năng chứa các vi phạm.

2.1.3 Phương pháp phân tích biến VRK

Phần này giới thiệu sơ lược về phương pháp phân tích biến VRK [19]. Đây là một phương pháp để tạo ra mô hình trừu tượng. Bài báo [19] áp dụng ý tưởng giải thuật PageRank vào phân tích biến để tính độ quan trọng của biến trong đồ thị phụ thuộc biến (xem Hình 2).



Hình 2: Đồ thị phụ thuộc biến[18]

Giải thuật phân tích biến hội tụ VRK được mô tả như sau:

a. Áp dụng giải thuật PageRank để tính toán độ quan trọng của mỗi biến trong đồ thị:

$$PR(A) = \frac{(1-d)}{N} + d\left(\sum_{B \in Parent(A)} \frac{PR(B)}{N(B)}\right)$$

N là số lượng biến, *Parent(A)* là một tập tất cả các biến mà A phụ thuộc vào, *N(B)* là số lượng các biến bị phụ thuộc vào B,d là hệ số damping được thiết lập giá trị giữa 0 và 1. Theo Brin *et al.* [1], giá trị tốt nhất cho d là 0.85.

b. Điều chỉnh mức độ quan trọng của biến có được từ bước i

Dựa vào mức (level) của biến trên đồ thị, thực hiện điều chỉnh lại độ quan trong của biến theo công thức sau:

$$E(x) = E(x) + \frac{MaxLevel - Level(x)}{MaxLevel}$$

MaxLevel là giá trị lớn nhất của level có trong đồ thị, *Level(x)* là level của biến x trên đồ thị.

2.2 Giải thuật đề xuất

Dựa trên giải thuật *đa trừu tượng* và *CEGAR*, chúng tôi đề xuất một phương pháp mới với ưu điểm của cả hai. Với *CEGAR*, bất cứ khi nào một counter-example được tìm thấy trên các mô hình trừu tượng, nó sẽ được tinh lọc trên hệ thống gốc. Với *đa trừu tượng*, việc tìm kiếm sẽ được thực hiện trên mô hình trừu tượng kế tiếp (theo mức độ trừu tượng của các mô hình giảm dần) mỗi khi lỗi được tìm thấy trên các mô hình trừu tượng trước, quá trình tìm kiếm không sử dụng lại thông tin về lỗi ở mô hình trước, đây cũng chính là nhược điểm của giải thuật. Giải thuật mới vận dụng ý tưởng *đa trừu tượng* từ [13] và *tinh lọc* counter-example từ CEGAR [4].

Giống như *đa trừu tượng*, giải thuật mới sẽ duyệt lần lượt qua một chuỗi các mô hình trừu tượng $M_0 \subseteq M_1 \subseteq \ldots$, để tìm kiếm các vi phạm (mức độ trừu tượng M_0 là nhiều nhất). Counter-example tìm thấy trên M_0 sẽ được xác nhận lại trên M_1 và tiếp tục theo thứ tự mức độ trừu tượng M_2, M_3...và sau đó là trên hệ thống gốc. Counter-example tìm thấy trên hệ thống gốc là một chứng cứ cho việc vi phạm các thuộc tính cần kiểm tra.

Một chuỗi quá trình kiểm tra có thể được kết thúc sớm hơn nếu counter-example không được xác nhận lại trên bất cứ mô hình trừu tượng M_i nào (kể cả mô hình gốc). Trong trường hợp này, lỗi được tìm thấy trên M_0 sẽ bị từ chối (vì M_i xác nhận