Chương 1

Mở đầu

Nội dung

- Automata
- Tập hợp
- Các phương pháp chứng minh hình thức
- Tóm tắt

Lý thuyết automata

- Lý thuyết automata nghiên cứu về những thiết bị tính toán trừu tượng - máy tính
- 1930s, A. Turing nghiên cứu về những máy tính trừu tượng có khả năng tính toán như những máy tính hiện nay
- 1940-1950s, nhiều nghiên cứu về các máy tính đơn giản
- 1969, S. Cook mở rộng nghiên cứu của Turing: cái gì có thể tính toán, cái gì không thể

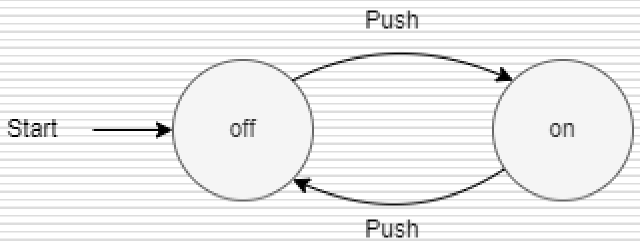
Vai trò

- Dùng trong thiết kế một số loại phần mềm
- Có thể hiểu cái ta có thể mong đợi từ phần mềm
- Giải quyết một số bài toán bằng những phương án xấp xỉ (heuristic)

Ứng dụng

- Thiết kế và kiểm chứng các mạch số
- Xây dựng bộ phân tích từ vựng của các trình biên dịch
- Tìm kiếm văn bản
- Kiểm chứng các hệ thống có số trạng thái là hữu hạn

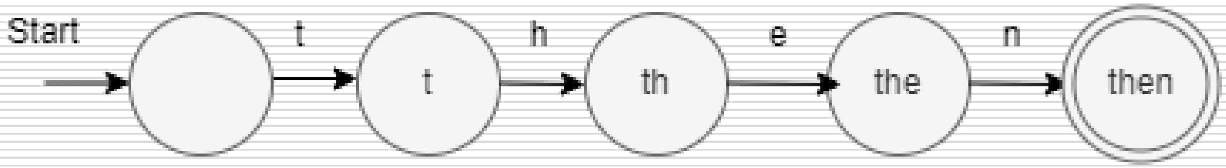
Ví dụ công tắc



- Trạng thái (state)
  - off, on
- Đầu vào (Input)
  - Push
- Bảng chuyển trạng thái (Transition table)

	Push
off	on
on	off

Ví dụ nhận biết từ khóa



- Có 5 trạng thái
  - Một trạng thái bắt đầu
  - Một hay nhiều kết thúc (chấp nhận)
- Đầu vào là ký tự

Thể hiện của automata

- Văn phạm: mô hình hỗ trợ việc thiết kế phần mềm xử lý dữ liệu dạng đệ quy
  - E → E + E
- Biểu thức chính quy: mô tả cấu trúc của văn bản (text)
  - ‘[A-Z][a-z]*[][A-Z][a-z]*’

Nội dung

- Automata
- Tập hợp
- Các phương pháp chứng minh hình thức
- Tóm tắt

Tập hợp

- Một tập hợp là một tổ hợp nhiều đối tượng (thành viên, phần tử)
  - $\forall x$ và tập hợp S.
    - $x \in S$: x là thành viên của S
    - $x \notin S$: x không là thành viên của S
  - Hai tập hợp A và B được gọi là bằng nhau (A=B) nếu mọi phần tử của A đều là thành viên của B và ngược lại

Mô tả

- Liệt kê các phần tử
  - Ví dụ:
    - {1, 4, 9, 16, 25}
    - {0, …, n}
    - N = {0, 1, 2, …}
  - Lực lượng của tập hợp A: $\|A\|$ số phần tử của A
    - $\|\{1,4,9,16,25\}\| = 5$

- Đặc tả tính chất đặc trưng: {<Biểu thức>|<Tính chất>}
  - Bình phương các số nguyên từ 1 đến 5:

$$\{x^2 \mid x \in Z \wedge 1 \leq x \leq 5\}$$

Tập con và tập rỗng

- Tập hợp A được gọi là tập hợp con của B, ký hiệu $A \subseteq B$, nếu và chỉ nếu mọi phần tử của A đều là thành viên của B
  - $A \nsubseteq B$: A không là tập con của B - có ít nhất 1 phần tử của A không thuộc B
- Tập hợp rỗng: tập hợp không có phần tử - $\emptyset$ ({})
  - $\emptyset = \{\} = \{x \mid 0=1\}$
- Cho 3 tập hợp A, B, C
  - $\emptyset \in A$
  - $A \subseteq A$ (quan hệ phản xạ)
  - Nếu $A \subseteq B$ và $B \subseteq C$ thì $A \subseteq C$ (quan hệ bắc cầu)
  - Nếu $A \subseteq B$ và $B \subseteq A$ thì $A = B$ (quan hệ phản xứng)

Các phép toán trên tập hợp

- Phép toán hợp
  - $A \cup B := \{z \mid z \in A \vee z \in B\}$
- Phép toán giao
  - $A \cap B := \{z \mid z \in A \wedge z \in B\}$
- Phép toán trừ
  - $A - B := \{z \mid z \in A \wedge z \notin B\}$
- sd

Tích Descartes

- Cho 2 đối tượng a và b, ta có thể tạo thành 1 cặp thứ tự, ký hiệu (a, b), như là một đối tượng riêng lẻ
  - $(a, b) \neq (b, a)$
  - Phân biệt (a, b) với {a, b} - cặp không thứ tự
- Tích Descartes của 2 tập hợp A và B
  - $A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$
  - $\{1, 2, 3\} \times \{a, b\} = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$

Quan hệ

- Cho 2 tập hợp A và B, một quan hệ (hai ngôi) đi từ A tới B là tập con R của AxB với
  - $R = \{(a, b) \mid \forall a \in A \wedge \forall b \in B\}$
- Cho S = {0, 1, 2, 3}
  - Quan hệ "thứ tự nhỏ hơn"
    - L = {(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)}
  - Quan hệ "bằng"
    - E = {(0, 0), (1, 1), (2, 2), (3, 3)}
  - Quan hệ chẵn lẻ
    - P = {(0, 0), (1, 1), (2, 2), (3, 3), (0, 2), (2, 0), (1, 3), (3, 1)}

Các tính chất của quan hệ

- Cho tập hợp, mối quan hệ
  - Phản xạ: $R = \{(a, a) \mid \forall a \in A\}$
  - Đối xứng: aRb --> bRa
  - Bắc cầu: aRb, bRc --> aRc
- Quan hệ tương đương: gồm quan hệ phản xạ, đối xứng và bắc cầu

Bao đóng của quan hệ

- P-closure = quan hệ nhỏ nhất thỏa các tính chất trong P
- Bao đóng bắc cầu R+
  - Nếu (a, b) ∈ R thì (a, b) ∈ R+
  - Nếu (a, b) ∈ R và (b, c) ∈ R thì (a, c) ∈ R+
  - Không còn gì để thêm trong R+
- Bao đóng phản xạ và bắc cầu
  - $R^* = R^+ \cup \{(a, a) | a \in A\}$
- Ví dụ: R = {(1, 2), (2, 2), (2, 3)} trên A = {1, 2, 3}
  - R+ = {(1, 2), (2, 2), (2, 3), (1, 3)}
  - R* = {(1, 2), (2, 2), (2, 3), (1, 3), (1, 1), (3, 3)}

Hàm

- Một quan hệ f đi từ A đến B được gọi là 1 hàm ánh xạ A vào B nếu và chỉ nếu với mỗi a∈ A có duy nhất b∈B để (a, b)∈ f.
  - Ký hiệu: f: A →B

Nội dung

- Automata
- Tập hợp
- Các phương pháp chứng minh hình thức
  - Trực tiếp
  - Phản chứng
  - Phản ví dụ
  - Quy nạp
- Tóm tắt

Định nghĩa, định lý, chứng minh

- Định nghĩa: mô tả các đối tượng và ký hiệu được sử dụng
  - Sau khi định nghĩa về các đối tượng và ký hiệu, có các phát biểu toán học về chúng
- Chứng minh: dùng lý lẽ logic thuyết phục một phát biểu là đúng
- Định lý: phát biểu toán học được chứng minh là đúng

Chứng minh trực tiếp

- Chứa một chuỗi các phát biểu mà chân trị bắt đầu từ các phát biểu ban đầu, gọi là giả thuyết, diễn giải logic đến các phát biểu tiếp theo, rồi đến phát biểu kết luận
- Định lý: Nếu $x \geq 4$ thì $2^x \geq x^2$
- Định lý: Nếu x là tổng bình phương của 4 số nguyên dương thì $2^x \geq x^2$

Rút về định nghĩa

- Nếu không biết bắt đầu chứng minh từ đâu, chuyển các giả thuyết về định nghĩa của chúng
- Chẳng hạn
  - Tập hợp S được gọi là hữu hạn nếu tồn tại số nguyên n sao cho S có đúng n phần tử: $||S|| = n$
    - Nếu S không hữu hạn, ta gọi S là tập vô hạn
  - Nếu S và T là 2 tập con của U, S được gọi là phần bù của T trong U nếu S∪T = U và S∩T=∅
- Định lý: Nếu S là một tập con hữu hạn của tập vô hạn U nào đó. Gọi T là phần bù của S trong U, lúc đó T là vô hạn

Nội dung

- Automata
- Tập hợp
- Các phương pháp chứng minh hình thức
  - Diễn dịch
  - Phản chứng
  - Phản ví dụ
  - Quy nạp
- Tóm tắt

Rút về định nghĩa

Phát biểu gốc	Phát biểu mới
S là hữu hạn	Tồn tại số nguyên n sao cho $\|S\| = n$
U là vô hạn	Không có số nguyên p nào để $\|U\| = p$
T là phần bù của S trong U	S∪T = U và S∩T=∅

- Giả sử T là hữu hạn → tồn tại số nguyên m: $\|T\| = m$
  - Lại có S ∪ T = U và S∩T=∅
    → Có m+n phần tử trong U: $\|U\| = m + n$
  - Do đó U là hữu hạn → trái với giả thuyết.
- Vậy T là vô hạn

Chứng minh phản chứng

- Chứng minh nếu H thì C
  - Bắt đầu với H và $\neg$C
  - Chỉ ra chỗ sai nếu bắt đầu với H và $\neg$C

Nội dung

- Automata
- Tập hợp
- Các phương pháp chứng minh hình thức
  - Diễn dịch
  - Phản chứng
  - Phản ví dụ
  - Quy nạp
- Tóm tắt

Phản ví dụ

- Gặp vấn đề dường như là đúng và cần xác định định lý là đúng hay sai.
  - Tìm cách chứng minh là đúng, nếu không thể, tìm ví dụ để đó không phải là định lý .
- Ví dụ: Tất cả các số nguyên tố đều là số lẻ
  - Phản ví dụ: 2 là số chẵn
- Ví dụ: Không có cặp số nguyên nào để a%b=b%a
  - Phản ví dụ: a=b=2 thì a%b = b%a = 0

Nội dung

- Automata
- Tập hợp
- Các phương pháp chứng minh hình thức
  - Diễn dịch
  - Phản chứng
  - Phản ví dụ
  - Quy nạp
- Tóm tắt

Nguyên lý quy nạp

- Bước 1 (cơ sở): chứng minh P(0)
- Bước 2 (giả thuyết quy nạp): giả sử P(n-1)
- Bước 3 (quy nạp): P(n-1) ➔ P(n) ∀n≥1

- Ví dụ: ∀n≥0, chứng minh $\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

Nội dung

- Automata
- Tập hợp
- Các phương pháp chứng minh hình thức
  - Diễn dịch
  - Phản chứng
  - Phản ví dụ
  - Quy nạp
- Tóm tắt

Tóm tắt

- Lý thuyết automata liên quan đến các phát biểu và thuộc tính toán học của các mô hình tính toán
  - Ứng dụng trong nhiều lĩnh vực
- Phương pháp chứng minh hình thức hỗ trợ việc xác minh tính đúng đắn của chương trình