# chương 2

# Chỉ định đồng hồ đơn giản

## 2.1 Hành vi

Trước khi cố gắng xác định một hệ thống, chúng ta hãy xem các nhà khoa học thực hiện nó như thế nào. Trong nhiều thế kỷ, họ đã mô tả một hệ thống với các phương trình xác định trạng thái của nó tiến triển như thế nào theo thời gian, trong đó trạng thái bao gồm các giá trị của các biến. Ví dụ, trạng thái của hệ bao gồm trái đất và mặt trăng có thể được mô tả bằng các giá trị của bốn biến e pos, m pos, e vel và m vel, biểu thị vị trí và vận tốc của hai vật thể. Các giá trị này là các phần tử trong không gian 3 chiều. Hệ thống trái đất-mặt trăng được mô tả bằng các phương trình biểu thị các giá trị của các biến dưới dạng hàm của thời gian và các hằng số nhất định—cụ thể là khối lượng, vị trí và vận tốc ban đầu của chúng.

Một hành vi của hệ thống trái đất-mặt trăng bao gồm hàm F theo thời gian đến các trạng thái, F(t) biểu thị trạng thái của hệ thống tại thời điểm t. Một hệ thống máy tính khác với các hệ thống được các nhà khoa học nghiên cứu theo truyền thống vì chúng ta có thể giả vờ rằng trạng thái của nó thay đổi theo từng bước riêng biệt. Vì vậy, chúng ta biểu diễn việc thực thi một hệ thống như một chuỗi các trạng thái. Về mặt hình thức, chúng ta định nghĩa một hành vi là một chuỗi các trạng thái, trong đó trạng thái là sự gán giá trị cho các biến. Chúng tôi chỉ định một hệ thống bằng cách chỉ định một tập hợp các hành vi có thể xảy ra—những hành vi thể hiện việc thực thi chính xác của hệ thống.

## 2.2 Đồng hồ một giờ

Hãy bắt đầu với một hệ thống rất đơn giản—một chiếc đồng hồ kỹ thuật số chỉ hiển thị giờ. Để làm cho hệ thống hoàn toàn tầm thường, chúng ta bỏ qua mối quan hệ giữa màn hình và thời gian thực tế. Khi đó, đồng hồ giờ chỉ là một thiết bị có màn hình hiển thị tuần hoàn từ các giá trị từ 1 đến 12. Giả sử biến hr đại diện cho đồng hồ.

trưng bày. Một hành vi điển hình của đồng hồ là trình tự

(2.1) [giờ = 11] [giờ = 12] [giờ = 1] [giờ = 2] · · ·

trong số các trạng thái, trong đó [hr = 11] là trạng thái trong đó biến hr có giá trị 11.
Một cặp trạng thái liên tiếp, chẳng hạn như [hr = 1] [hr = 2], được gọi là một bước.

Để chỉ định đồng hồ giờ, chúng tôi mô tả tất cả các hành vi có thể có của nó. Chúng tôi viết một vị từ ban đầu chỉ định các giá trị ban đầu có thể có của mối quan hệ hr chỉ , một trạng thái tiếp theo định cách giá trị của hr có thể thay đổi trong bất kỳ bước nào.

Chúng tôi không muốn chỉ định chính xác những gì màn hình hiển thị ban đầu; bất cứ giờ nào cũng được. Vì vậy, chúng ta muốn vị từ ban đầu khẳng định rằng hr có thể có bất kỳ giá trị nào từ 1 đến 12. Hãy gọi vị từ ban đầu là HCini. Chúng ta có thể định nghĩa HCini một cách không chính thức bằng cách

Ký hiệu có = nghĩa là được định nghĩa bằng nhau.

HCini = giờ {1, . . . , 12}

Sau này, chúng ta sẽ xem cách viết định nghĩa này một cách chính thức mà không cần có ". . . " nghĩa là không chính thức, v.v.

Quan hệ trạng thái tiếp theo HCnxt là công thức biểu diễn mối quan hệ giữa các giá trị của hr ở trạng thái cũ (thứ nhất) và trạng thái mới (thứ hai) của một bước. Chúng ta đặt hr đại diện cho giá trị của hr ở trạng thái cũ và hr đại diện cho giá trị của nó ở trạng thái mới. (In hr được đọc là số nguyên tố.) Chúng ta muốn quan hệ trạng thái tiếp theo khẳng định rằng hr bằng hr + 1 ngoại trừ nếu hr bằng 12, trong trường hợp đó hr sẽ bằng 1. Sử dụng cấu trúc if/then/else với ý nghĩa rõ ràng , chúng ta có thể định nghĩa HCnxt là quan hệ trạng thái tiếp theo bằng cách viết

HCnxt = hr = nếu hr = 12 thì hr + 1 còn lại 1

HCnxt là một công thức toán học thông thường, ngoại trừ việc nó chứa các biến có sẵn cũng như không có sẵn. Một công thức như vậy được gọi là một hành động. Một hành động là đúng hoặc sai của một bước. Bước thỏa mãn hành động HCnxt được gọi là bước HCnxt.

Khi một bước HCnxt xảy ra, đôi khi chúng ta nói rằng HCnxt đã được thực thi.
Tuy nhiên, sẽ là một sai lầm nếu coi trọng thuật ngữ này. Một hành động là một công thức và các công thức không được thực thi.

Chúng tôi muốn đặc tả của chúng tôi là một công thức duy nhất, không phải là cặp công thức HCini và HCnxt. Công thức này phải khẳng định một hành vi (i) trạng thái ban đầu của nó thỏa mãn HCini, và (ii) mỗi bước của nó thỏa mãn HCnxt. Chúng tôi biểu thị (i) dưới dạng công thức HCini, mà chúng tôi hiểu là một tuyên bố về hành vi có nghĩa là trạng thái ban đầu thỏa mãn HCini. Để diễn đạt (ii), chúng ta sử dụng toán tử logic thời gian (phát âm là hộp ). Công thức thời gian F khẳng định công thức F luôn đúng. Đặc biệt, HCnxt là khẳng định rằng HCnxt đúng cho mọi bước trong hành vi. Vì vậy, HCini HCnxt đúng với một hành vi nếu trạng thái ban đầu thỏa mãn HCini và mọi bước đều thỏa mãn HCnxt. Công thức này mô tả tất cả các hành vi giống như trong (2.1) trên trang này; có vẻ như đó là thông số kỹ thuật mà chúng tôi đang tìm kiếm.

Nếu chúng ta chỉ xem xét đồng hồ một cách riêng biệt và không bao giờ cố gắng liên hệ nó với một hệ thống khác thì đây sẽ là một thông số kỹ thuật tốt. Tuy nhiên, giả sử đồng hồ là một phần của hệ thống lớn hơn—ví dụ: màn hình hiển thị giờ của trạm thời tiết hiển thị giờ và nhiệt độ hiện tại. Trạng thái của trạm được mô tả bằng hai biến: hr, biểu thị hiển thị giờ và tmp, biểu thị hiển thị nhiệt độ. Hãy xem xét hành vi này của trạm thời tiết:

giờ = 11 giờ = 12 giờ = 12
tmp = 23,5 tmp = 23,5 tmp = 23,4

giờ = 12 giờ = 1
tmp = 23,3 tmp = 23,3

. . .

Ở bước thứ hai và thứ ba, tmp thay đổi nhưng hr vẫn giữ nguyên. Các bước này không được HCnxt cho phép, điều này khẳng định rằng mỗi bước phải tăng hr .
Công thức HCini HCnxt không mô tả đồng hồ giờ ở trạm thời tiết.

Một công thức mô tả bất kỳ đồng hồ giờ nào cũng phải cho phép các bước không thay đổi giờ—nói cách khác, các bước hr = hr. Đây được gọi là các bước nói lắp của đồng hồ. Đặc điểm kỹ thuật của đồng hồ giờ phải cho phép cả bước HCnxt và bước lặp. Vì vậy, một bước sẽ được cho phép nếu đó là bước HCnxt hoặc bước lắp ghép—nghĩa là, nếu đó là bước thỏa mãn HCnxt (hr = hr ). Điều này gợi ý rằng chúng tôi áp dụng HCini (HCnxt (hr = hr )) làm thông số kỹ thuật của mình.
Trong TLA, chúng ta đề [HCnxt]hr là viết tắt của Hcnxt (hr = hr ), vì vậy chúng ta có thể viết dưới dạng công thức gọn hơn như HCini [HCnxt]hr .

chữ I phát âm [HCnxt]hr

hình vuông HCnxt phụ hr.

Công thức HCini [HCnxt]hr cho phép các bước lặp. Trong thực tế, nó cho phép hành vi

[giờ = 10] [giờ = 11] [giờ = 11] [giờ = 11] · · ·

kết thúc bằng một chuỗi vô tận các bước nói lắp. Hành vi này mô tả một chiếc đồng hồ có màn hình hiển thị đạt giá trị 11 và sau đó giữ giá trị đó mãi mãi—nói cách khác, một chiếc đồng hồ dừng ở 11. Theo cách tương tự, chúng ta có thể biểu diễn việc kết thúc thực thi của bất kỳ hệ thống nào bằng một hành vi vô hạn kết thúc bằng một chuỗi không có gì ngoài những bước lắp bắp. Chúng ta không cần những hành vi hữu hạn (chuỗi hữu hạn các trạng thái), vì vậy chúng ta chỉ xem xét những hành vi vô hạn.

Việc yêu cầu đồng hồ không dừng là điều tự nhiên, vì vậy đặc tả của chúng tôi phải khẳng định rằng có vô số bước không bị lặp. Chương 8 giải thích cách thể hiện yêu cầu này. Hiện tại, chúng ta hài lòng với những chiếc đồng hồ có thể dừng và chúng ta coi thông số kỹ thuật của đồng hồ giờ là công thức HC được xác định bởi

HC = HCini [HCnxt]giờ

## 2.3 Xem xét kỹ hơn về đặc điểm kỹ thuật

Trạng thái là sự gán giá trị cho các biến, nhưng biến nào? Câu trả lời rất đơn giản: tất cả các biến. Trong hành vi (2.1) ở trang 16, [hr = 1] thể hiện một số trạng thái cụ thể gán giá trị 1 cho hr . Nó có thể gán giá trị 23 cho biến tmp và giá trị √ 17 cho biến m pos. Chúng ta có thể coi một trạng thái là đại diện cho một trạng thái tiềm năng của toàn bộ vũ trụ. Trạng thái gán 1 cho giờ và một điểm cụ thể trong không gian 3 cho m pos mô tả trạng thái của vũ trụ trong đó đồng hồ giờ chỉ 1 và mặt trăng ở một vị trí cụ thể.

Trạng thái gán √ 2 cho giờ không tương ứng với bất kỳ trạng thái nào của vũ trụ mà chúng ta nhận ra, vì đồng hồ giờ không thể hiển thị giá trị √ 2. Nó có thể đại diện cho trạng thái của vũ trụ sau khi một quả bom rơi xuống đồng hồ, khiến cho việc hiển thị nó hoàn toàn là tưởng tượng.

Một hành vi là một chuỗi vô hạn các trạng thái—ví dụ:

(2.2) [giờ = 11] [giờ = 77,2] [giờ = 78,2] [giờ = √ 2] . . .

Một hành vi mô tả một lịch sử tiềm năng của vũ trụ. Hành vi (2.2) không tương ứng với lịch sử mà chúng tôi hiểu, vì chúng tôi không biết cách hiển thị đồng hồ có thể thay đổi từ 11 thành 77,2. Dù nó đại diện cho loại lịch sử nào thì cũng không phải là lịch sử mà đồng hồ đang làm những gì nó phải làm.

Công thức HC là công thức thời gian. Công thức thời gian là một sự khẳng định về hành vi. Chúng ta nói rằng một hành vi thỏa mãn HC nếu HC là một khẳng định đúng về hành vi đó. Hành vi (2.1) thỏa mãn công thức HC . Hành vi (2.2) thì không, vì HC khẳng định rằng mọi bước đều thỏa mãn HCnxt hoặc giữ nguyên hr, còn bước đầu tiên và bước thứ ba của (2.2) thì không. (Bước thứ hai, [hr = 77,2] [hr = 78,2], thỏa mãn HCnxt.) Chúng ta coi công thức HC là đặc điểm kỹ thuật của đồng hồ giờ vì nó thỏa mãn chính xác những hành vi biểu thị lịch sử của vũ trụ trong đó đồng hồ hoạt động bình thường.

Nếu đồng hồ hoạt động bình thường thì màn hình hiển thị của nó phải là số nguyên từ 1 đến 12. Vì vậy, hr phải là số nguyên từ 1 đến 12 trong mọi trạng thái của bất kỳ hành vi nào thỏa mãn đặc điểm kỹ thuật của đồng hồ, HC . Công thức HCini khẳng định rằng hr là số nguyên từ 1 đến 12, và HCini khẳng định rằng HCini luôn đúng. Vì vậy, HCini phải đúng với mọi hành vi thỏa mãn HC . Một cách khác để nói điều này là HC ngụ ý HCini, cho mọi hành vi. Như vậy, công thức HC HCini phải được thỏa mãn với mọi hành vi. Một công thức thời gian thỏa mãn mọi hành vi được gọi là một định lý, vì vậy HC HCini phải là một định lý.[1] Dễ dàng thấy rằng: HC ngụ ý rằng HCini ban đầu đúng (ở trạng thái đầu tiên của hành vi) và [HCnxt]hr ngụ ý rằng mỗi bước sẽ tăng hr tới giá trị tiếp theo phù hợp của nó hoặc nếu không thì giữ nguyên hr. Chúng ta có thể hình thức hóa lý luận này bằng cách sử dụng các quy tắc chứng minh của TLA, nhưng chúng ta sẽ không đi sâu vào chứng minh và các quy tắc chứng minh.

[1] Các nhà logic học gọi một công thức là hợp lệ nếu nó được mọi hành vi thỏa mãn; họ bảo lưu định lý thuật ngữ cho các công thức có giá trị có thể chứng minh được.

## 2.4 Thông số kỹ thuật trong TLA+

Hình 2.1 trên trang tiếp theo cho thấy cách viết thông số kỹ thuật về đồng hồ giờ bằng TLA+. Có hai phiên bản: phiên bản ascii ở phía dưới là thông số kỹ thuật TLA+ thực tế, cách bạn nhập nó; phiên bản sắp chữ ở trên cùng là phiên bản mà chương trình TLATEX, được mô tả trong Chương 13, có thể tạo ra. Trước khi cố gắng hiểu đặc tả, hãy quan sát mối quan hệ giữa hai cú pháp.

- Các từ dành riêng xuất hiện bằng chữ in hoa nhỏ (như mở rộng) được viết bằng ascii với chữ in hoa thông thường.
- Khi có thể, các ký hiệu được thể hiện bằng hình ảnh trong ascii—ví dụ: được gõ là [ ] và = là #. (Bạn cũng có thể gõ = dưới dạng /=.)
- Khi không có cách trình bày ascii tốt, ký hiệu TEX2 sẽ được sử dụng—ví dụ: được gõ là \in. Ngoại lệ chính là =, được gõ là = = .

Danh sách đầy đủ các ký hiệu và ascii tương đương của chúng xuất hiện trong Bảng 8 trên trang 273. Tôi thường sẽ hiển thị phiên bản sắp chữ của một thông số kỹ thuật; Bạn có thể tìm thấy phiên bản ascii của tất cả các thông số kỹ thuật trong cuốn sách này thông qua trang Web TLA.

Bây giờ hãy xem thông số kỹ thuật nói gì. Nó bắt đầu với

mô-đun GiờĐồng hồ

bắt đầu một mô-đun có tên HourClock. Thông số kỹ thuật TLA+ được phân chia thành các mô-đun; đặc điểm kỹ thuật của đồng hồ giờ bao gồm mô-đun duy nhất này.

Các toán tử số học như + không được tích hợp vào TLA+ mà được xác định trong các mô-đun. (Bạn có thể muốn viết một đặc tả trong đó + có nghĩa là phép cộng các ma trận thay vì số.) Các toán tử thông thường trên số tự nhiên được xác định trong mô-đun Naturals. Định nghĩa của chúng được tích hợp vào mô-đun HourClock bằng câu lệnh

mở rộng Naturals

Mọi ký hiệu xuất hiện trong công thức phải là toán tử tích hợp của TLA+ hoặc phải được khai báo hoặc xác định. Tuyên bố

biến giờ

tuyên bố hr là một biến.

2Hệ thống sắp chữ TEX được mô tả trong The TEXbook của Donald E. Knuth, được xuất bản bởi Addison-Wesley, Reading, Massachusetts, 1986.

mô-đun GiờĐồng hồ

mở rộng Naturals

biến giờ

HCini = giờ (1 . . 12)

HCnxt = hr = nếu hr = 12 thì hr + 1 còn lại 1 HC =

HCini [HCnxt]hr

định lý HC HCini

---------- MODULE Đồng hồ giờ ---------- MỞ RỘNG Naturals BIẾN GIỜ HCini ==
giờ \in (1 .. 12)

HCnxt == hr' = IF hr # 12 THEN hr + 1 ELSE 1 HC == HCini /\ []
[HCnxt]_hr

Định lý HC => []HCini
==========

Hình 2.1: Đặc tả đồng hồ giờ—bộ sắp chữ và phiên bản ASCII.

Để định nghĩa HCini, chúng ta cần biểu diễn tập {1, . . . , 12} chính thức, không có dấu chấm lửng ". . .". Chúng ta có thể viết điều này hoàn toàn dưới dạng

{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}

nhưng điều đó thật mệt mỏi. Thay vào đó, chúng tôi sử dụng toán tử ". .", được xác định trong mô-đun Naturals, để viết tập hợp này là 1 . . 12. Nói chung tôi . . j là tập hợp các số nguyên từ i đến j, với mọi số nguyên i và j. (Nó bằng tập rỗng nếu j < i.) Bây giờ ta đã rõ cách viết định nghĩa của HCini. Các định nghĩa về HCnxt và HC được viết giống như trước đây. (Các toán tử thông thường của logic và lý thuyết tập hợp, như và , được tích hợp vào TLA+.)

Dòng

có thể xuất hiện ở bất cứ đâu giữa các câu lệnh; nó hoàn toàn chỉ là mỹ phẩm và không có ý nghĩa gì. Sau đó là lời phát biểu

định lý HC HCini

của định lý đã được thảo luận ở trên. Tuyên bố này khẳng định rằng công thức HC HCini là đúng trong bối cảnh của tuyên bố. Chính xác hơn, nó

khẳng định rằng công thức tuân theo một cách hợp lý các định nghĩa trong mô-đun này, các định nghĩa trong mô-đun Naturals và các quy tắc của TLA+. Nếu công thức không đúng thì mô-đun sẽ sai.

Mô-đun được kết thúc bằng ký hiệu

Đặc tả của đồng hồ giờ là định nghĩa của HC, bao gồm định nghĩa về các công thức HCnxt và HCini và các toán tử. . và + xuất hiện trong định nghĩa của HC . Về mặt hình thức, không có gì trong mô-đun cho chúng ta biết rằng HC chứ không phải HCini là thông số kỹ thuật của đồng hồ. TLA+ là ngôn ngữ để viết toán học—đặc biệt là để viết các định lý và định nghĩa toán học. Những định nghĩa đó thể hiện điều gì và ý nghĩa mà chúng tôi gán cho các định lý đó nằm ngoài phạm vi toán học và do đó nằm ngoài phạm vi của TLA+. Kỹ thuật không chỉ đòi hỏi khả năng sử dụng toán học mà còn là khả năng hiểu được những gì toán học cho chúng ta biết về một hệ thống thực tế, nếu có.

## 2.5 Thông số kỹ thuật thay thế

Mô-đun Naturals cũng xác định toán tử mô đun mà chúng tôi viết %. Công thức i % n, mà các nhà toán học viết i mod n, là số dư khi chia i cho n. Chính thức hơn, i % n là số tự nhiên nhỏ hơn n thỏa mãn i = q n + (i % n) đối với một số tự nhiên q. Hãy biểu diễn điều kiện này bằng toán học. Mô-đun Naturals định nghĩa Nat là tập hợp các số tự nhiên và khẳng định tồn tại aq trong tập hợp Nat thỏa mãn công thức F được viết q Nat : F. Do đó, nếu i và n là các phần tử của Nat và n > 0 thì i % n là số duy nhất thỏa mãn

(i % n 0 . . (n 1)) ( q Nat : i = q n + (i % n))

Chúng ta có thể sử dụng % để đơn giản hóa thông số đồng hồ giờ một chút. Quan sát thấy (11 % 12)+1 bằng 12 và (12 % 12)+1 bằng 1, chúng ta có thể định nghĩa một hành động trạng thái tiếp theo khác HCnxt2 và một công thức khác HC 2 là thông số kỹ thuật của đồng hồ

HCnxt2 = giờ = (giờ % 12) + 1 HC 2 = HCini [HCnxt2]giờ

Hành động HCnxt và HCnxt2 không tương đương. Bước [hr = 24] [hr = 25] thỏa mãn HCnxt nhưng không thỏa mãn HCnxt2, trong khi bước [hr = 24] [hr = 1] thỏa mãn HCnxt2 nhưng không thỏa mãn HCnxt. Tuy nhiên, bất kỳ bước nào cũng bắt đầu ở trạng thái có hr trong 1 . . 12 thỏa mãn HCnxt nếu nó thỏa mãn HCnxt2. Do đó, không khó để suy ra rằng bất kỳ hành vi nào bắt đầu ở trạng thái thỏa mãn HCini đều thỏa mãn [HCnxt]hr nếu nó thỏa mãn [HCnxt2]hr . Do đó, công thức HC và HC 2 là tương đương. Nói cách khác, HC ≡ HC 2 là một định lý. Việc chúng ta coi công thức nào trong hai công thức này là thông số kỹ thuật của đồng hồ giờ không quan trọng.

Toán học cung cấp vô số cách để diễn đạt cùng một điều. Các biểu thức 6 + 6, 3 4 và 141 129 đều có cùng một ý nghĩa; chúng chỉ là những cách viết khác nhau của số 12. Chúng ta có thể thay thế một trong hai trường hợp của số 12 trong mô-đun HourClock bằng bất kỳ biểu thức nào trong số này mà không làm thay đổi ý nghĩa của bất kỳ công thức nào của mô-đun.

Khi viết một đặc tả, bạn thường phải đối mặt với việc lựa chọn cách diễn đạt điều gì đó. Khi điều đó xảy ra, trước tiên bạn phải đảm bảo rằng các lựa chọn mang lại thông số kỹ thuật tương đương. Nếu đúng như vậy thì bạn có thể chọn cái mà bạn cảm thấy làm cho đặc tả dễ hiểu nhất. Nếu không, thì bạn phải quyết định xem bạn muốn nói đến cái nào.