

TÍNH KHẢ TUẦN TỰ CỦA GIAO THỨC ĐIỀU KHIỂN TƯƠNG TRANH KHÓA HAI PHA TRONG CƠ SỞ DỮ LIỆU THỜI GIAN THỰC

ĐOÀN VĂN BAN, HỒ VĂN HƯƠNG

Abstract. In this paper, we present a formal model of real time database system using Duration Calculus (DC). We give a formal specification of the correctness criterion for the execution of transaction systems and of the two phase locking concurrency control protocol (2PL-CCP). We also give a formal proof for the correctness of the 2PL-CCP using the DC proof systems.

Tóm tắt. Trong bài này, chúng tôi trình bày một mô hình hình thức của hệ thống cơ sở dữ liệu thời gian thực trong logic tính toán khoảng Duration Calculus (DC). Chúng tôi đưa ra đặc tả hình thức chính xác cho việc thực hiện của hệ thống các giao tác và giao thức điều khiển tương tranh khóa hai pha 2PL-CCP. Chúng tôi cũng đưa ra một chứng minh hình thức tính đúng của các giao thức điều khiển tương tranh khóa hai pha trong cơ sở dữ liệu thời gian thực sử dụng hệ thống chứng minh DC.

1. MỞ ĐẦU

Ngày nay các hệ thống thời gian thực (HTTGT) được đặc biệt quan tâm khi cần phải quản lý một khối lượng lớn dữ liệu và hỗn hợp. Hiệu quả của các thuật toán quản lý việc truy nhập và thao tác dữ liệu trong các HTTGT phụ thuộc nhiều vào điều kiện ràng buộc về thời gian của các ứng dụng đã được cung cấp.

Trong bài báo chúng tôi trình bày về một đặc tả hình thức điều khiển tương tranh của cơ sở dữ liệu thời gian thực (CSDLTGT) trong logic tính toán khoảng DC (Duration Calculus) [5, 10]. CSDLTGT có thể xem như là sự hợp nhất giữa cơ sở dữ liệu (CSDL) với HTTGT. Trước tiên giới thiệu tóm tắt đặc tả hình thức chính xác cho việc thực hiện của hệ thống các giao tác và giao thức điều khiển tương tranh khóa hai pha 2PL-CCP (Two Phase Locking Concurrency Control Protocol) [1, 9]. Sau đó là một chứng minh hình thức tính đúng của các giao thức điều khiển tương tranh trong CSDLTGT để khẳng định được tính đúng của hệ thống các giao tác đảm bảo hệ thống thực hiện nhất quán.

2. HỆ THỐNG CƠ SỞ DỮ LIỆU THỜI GIAN THỰC

Cơ sở dữ liệu là một hệ thống tích hợp các quan hệ dữ liệu về các tổ chức được lưu trữ trên máy tính. Việc truy nhập của người sử dụng tới CSDL được thực hiện thông qua các giao tác, đó là một dãy logic các thao tác chính là đọc và ghi.

Một giao thức đảm bảo thực hiện tính nguyên tử được gọi là giao thức CCP (Concurrency Control Protocol). Điều kiện để thực hiện tương tranh các giao tác trong CSDL đảm bảo tính nhất quán dữ liệu là khả năng tuần tự (serializability) [1, 4, 9]. CSDLTGT có thể xem như là sự kết hợp của CSDL và HTTGT. Điều kiện cần để tuần tự hóa được là các giao tác thực hiện các thao tác trong thời gian thực phải thỏa mãn cả ràng buộc thời gian trên các giao tác ủy thác thực hiện (gọi tắt là ủy thác) có thời hạn [1].

Trong CSDLTGT, tập các đối tượng dữ liệu bao gồm cả lâm thời (temporal) và phi lâm thời (non-temporal). Một đối tượng dữ liệu lâm thời phản ánh trạng thái của các đối tượng xuất hiện trong thế giới thực. Mỗi giá trị của một đối tượng dữ liệu lâm thời có thể hợp lệ và không hợp lệ trong một thời khoảng nào đó.

Có hai thể hiện khác nhau của đối tượng dữ liệu: thể hiện bên ngoài (thế giới thực) và thể

hiện trong CSDL. Chúng có quan hệ thời gian với nhau và điều này được gọi là tính nhất quán theo thời gian. Tính nhất quán theo thời gian được thể hiện theo hai khía cạnh: tuyệt đối và tương đối. Tính nhất quán tuyệt đối được thể hiện khi thực hiện những yêu cầu cần xem dữ liệu tức thì, dữ liệu mới nhất của hệ thống. Tính nhất quán tương đối theo thời gian thể hiện yêu cầu tương ứng về số lượng dữ liệu được sử dụng qua lại với nhau.

Trong CSDLTGT, xử lý giao tác rất phức tạp vì nó đòi hỏi phải tích hợp một tập lớn các giao thức sao cho không chỉ duy trì tính nhất quán của CSDL mà còn phải đảm bảo thao tác thỏa mãn các ràng buộc về thời gian. Đặc biệt, khi CSDLTGT yêu cầu một CCP mới, sẽ dẫn đến một yêu cầu cần xác định điểm tới hạn của thời gian và ràng buộc thời gian kết hợp với các giao tác cần thực hiện.

3. LOGIC TÍNH TOÁN KHOẢNG DC

Trong phần này chúng ta xét một số tính chất cơ bản của logic tính toán khoảng DC, một mô hình đặc tả hình thức cho các CSDL và CSDLTGT [5, 10].

Thời gian *Time* trong DC là tập R^+ các số thực không âm. Với $t, t' \in R^+$, $t \leq t'$, kí hiệu $[t, t']$ là thể hiện khoảng thời gian từ t tới t' .

Giả thiết E là tập các biến trạng thái logic nhận các giá trị logic 0 (*false*) hoặc 1 (*true*). Tập các biểu thức trạng thái SR được định nghĩa như sau:

1. Mỗi biến trạng thái $P \in E$ là một biểu thức trạng thái thuộc SR.
2. Nếu P và $Q \in SR$ thì $\neg P$, $(P \wedge Q)$, $(P \vee Q)$, $(P \Rightarrow Q)$, $(P \Leftrightarrow Q)$ cũng là các biểu thức thuộc SR.

Thể hiện của trạng thái P được xem như là một hàm $I(P) : R^+ \rightarrow \{0, 1\}$. $I(P)(t) = 1$ khẳng định trạng thái P có mặt tại thời điểm xác định t và $I(P)(t) = 0$ khẳng định trạng thái P không có mặt tại thời điểm t . Chúng ta giả thiết rằng mọi biến trạng thái đều có thể thay đổi hữu hạn lần trong một khoảng thời gian hữu hạn. Một biểu thức trạng thái được thể hiện như là một hàm và được định nghĩa bởi sự biến đổi trạng thái theo các toán tử logic.

Với biểu thức P xác định một khoảng tương ứng, kí hiệu là $\int P$ chính là tổng độ dài các khoảng thời gian trong đó P xác định. Cho trước thể hiện I xác định đối với biến trạng thái P trong khoảng $[t, t']$, thể hiện của thời khoảng $I(\int P)([t, t'])$ được định nghĩa là $\int_t^{t'} I(P)(t)dt$. Do đó $\int P$ luôn cho ta độ dài của các thời đoạn và được ký hiệu là L .

Công thức khoảng nguyên thủy là một biểu thức được tạo lập từ các hạng thức và các phép toán quan hệ trên các số thực như phép so sánh bằng $=$ và phép so sánh nhỏ hơn $<$. Công thức khoảng là công thức nguyên thủy hoặc biểu thức được xây dựng từ các công thức trên cơ sở dùng các phép toán logic $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, \cap$ hay các lượng tử \forall, \exists áp dụng vào các biến xác định trên R^+ .

Công thức khoảng D trong DC thỏa mãn thể hiện I trong thời khoảng $[t', t'']$ nếu nó nhận giá trị đúng dưới thể hiện I trong thời khoảng đó, sẽ được viết như sau: $I, [t' t''] \models D$. Trong đó thể hiện trạng thái I là hàm từ R^+ tới $\{0, 1\}$.

Cho trước một thể hiện I , công thức $D_1 \cap D_2$ đúng trong $[t', t'']$ nếu tồn tại thời điểm $t : t' \leq t \leq t''$ sao cho D_1, D_2 đúng trong $[t', t]$ và $[t, t'']$ tương ứng.

Sau đây chúng ta nhắc lại một số công thức khoảng sẽ được sử dụng trong các chứng minh về sau.

Với mỗi trạng thái P , $[P]$ kí hiệu cho một thời đoạn (không phải là các thời điểm) mà trong đó P xuất hiện. Như vậy

$$[P] = (\int P = L) \wedge (L > 0).$$

Ký hiệu $[]$ sử dụng cho tân từ nhận giá trị đúng cho những thời đoạn là các thời điểm.

Mở rộng các định nghĩa ta có:

$$[P]^* \cong [] \vee [P].$$

Tiếp theo là các thể thức \diamond - biểu diễn cho "thỉnh thoảng", \square - biểu diễn cho "luôn luôn", được định nghĩa sau:

$$\diamond D \cong true \cap D \cap true,$$

$$\square D \cong \neg \diamond \neg D.$$

$\diamond D$ có giá trị *true* (đúng) trong một thời đoạn nếu và chỉ nếu D đúng trong thời đoạn con nào đó của thời đoạn đó.

$\square D$ có giá trị *true* nếu và chỉ nếu D đúng trong mọi thời đoạn con của thời đoạn đó, nói cách khác là không khi nào D có giá trị *false* trong thời đoạn đó. Sau đây là một số luật, tiên đề quan trọng:

$$\text{if } A \Rightarrow B \text{ then } (A \cap C \Rightarrow B \cap C) \quad (\text{DC-1})$$

$$\text{if } A \Rightarrow B \text{ then } (C \cap A \Rightarrow C \cap B)$$

$$(A \cap B) \cap C \Leftrightarrow A \cap (B \cap C) \quad (\text{DC-2})$$

$$(A \cap []) \Leftrightarrow ([] \cap A) \Leftrightarrow A \quad (\text{DC-3})$$

$$(A \cap false) \Leftrightarrow (false \cap A) \Leftrightarrow false \quad (\text{DC-4})$$

$$(A \vee B) \cap C \Leftrightarrow (A \cap C) \vee (B \cap C)$$

$$C \cap (A \vee B) \Leftrightarrow (C \cap A) \vee (C \cap B) \quad (\text{DC-5})$$

$$(A \wedge B) \cap C \Rightarrow (A \cap C) \wedge (B \cap C)$$

$$C \cap (A \wedge B) \Rightarrow (C \cap A) \wedge (C \cap B) \quad (\text{DC-6})$$

$$\square A \Rightarrow A \quad (\text{DC-7})$$

$$[P] \cap [P] \Leftrightarrow [P] \quad (\text{DC-8})$$

$$[P] \Rightarrow \square([P] \ast) \quad (\text{DC-9})$$

$$[P] \wedge [Q] \Leftrightarrow [P \wedge Q] \quad (\text{DC-10})$$

$$[P] \cap true \wedge true \cap [\neg P] \Rightarrow [P] \cap true \cap [\neg P] \quad (\text{DC-11})$$

$$[P] \cap true \cap [\neg P] \Rightarrow [P] \cap [\neg P] \cap true \wedge true \cap [\neg P] \cap [P] \quad (\text{DC-12})$$

$$[P] \cap true \wedge true \cap [\neg P] \cap A \Rightarrow [P] \cap true \cap [\neg P] \cap A \quad (\text{DC-13})$$

$$A \cap [P] \cap true \wedge true \cap [\neg P] \Rightarrow A \cap [P] \cap true \cap [\neg P] \quad (\text{DC-14})$$

$$[P] \wedge [Q1] \cap [Q2] \Leftrightarrow ([P] \wedge [Q1]) \cap ([P] \wedge [Q2]) \quad (\text{DC-15})$$

$$[P] \cap ([\neg P] \wedge A) \wedge [P] \cap ([\neg P] \wedge B) \Rightarrow [P] \cap ([\neg P] \wedge A \wedge B) \quad (\text{DC-16})$$

$$\neg [P] \Leftrightarrow [] \vee \diamond [\neg P] \quad (\text{DC-17})$$

$$\square (A) \cap \square (B) \Rightarrow \square (A \vee B \vee A \cap B) \quad (\text{DC-18})$$

4. HÌNH THỨC HÓA HTCSDLTGT TRONG DC

4.1. Mô hình cơ bản

Như ở phần trên ta đã xét, CSDL gồm một tập θ các đối tượng dữ liệu (ký hiệu là x, y, z, \dots) và tập $T = \{T_i | i \leq n\}$ các giao tác. Mỗi giao tác T_i có thể thực hiện trong CSDL ở thời điểm χ_i không xác định trước. Khi thực hiện, giao tác đó có thể đọc Vw_i một số đối tượng dữ liệu, thực hiện một số tính toán riêng và sau đó có thể thực hiện một số thao tác ghi Wr_i trên cùng các đối tượng dữ liệu đó. Mỗi giao tác có thể đọc và ghi dữ liệu ngay trong quá trình thực hiện, và các thao tác đọc thực hiện trước các thao tác ghi.

$x \in \theta, i \leq n$, biến trạng thái $Wr_i(x)$ mô tả hành vi của đối tượng x . $Wr_i(x)$ đúng tại thời điểm t khi và chỉ khi giá trị của x được giao tác T_i thực hiện thao tác ghi ở thời điểm t . Như vậy

$$Wr_i \in \theta \rightarrow Time \rightarrow \{0, 1\},$$

$$Wr_i(x)(t) = 1 \Leftrightarrow T_i \text{ ghi giá trị cho } x \text{ tại thời điểm } t.$$

$Vw_i(x)$ xác định trạng thái đọc x của T_i .

$Vw_i(x)$ đúng ở thời điểm t khi và chỉ khi T_i thực hiện thao tác đọc được x trước thời điểm t .

$$Vw_i \in \theta \rightarrow Time \rightarrow \{0, 1\},$$

$$Vw_i(x)(t) = 1 \Leftrightarrow T_i \text{ thực hiện đọc được } x \text{ tại thời điểm } t.$$

Một giao tác có thể ủy thác (commit) hoặc hủy bỏ (abort). Với mỗi $i \leq n$ biến trạng thái cm_i và ab_i , được sử dụng để mô tả trạng thái được ủy thác và bị hủy bỏ (tương ứng) của giao tác T_i .

$cm_i, ab_i \in Time \rightarrow \{0, 1\}$,
 $cm_i(t) = 1 \Leftrightarrow T_i$ đã ủy thác trước thời điểm t ,
 $ab_i(t) = 1 \Leftrightarrow T_i$ bị hủy bỏ trước thời điểm t .

Vấn đề chính là cần đặc tả quá trình thực hiện các giao tác từ đầu tới thời điểm mà các giao tác được ủy thác hoặc bị hủy bỏ. Biểu thức trạng thái đó được xác định như sau:

$$F \cong \bigwedge_{i \leq n} (cm_i \vee ab_i).$$

Biểu trạng thái F nhận giá trị true ở thời điểm t nếu với mọi $i \leq n$, T_i hoặc được ủy thác hoặc bị hủy bỏ trước thời điểm t .

Các thời đoạn thể hiện toàn bộ quá trình thực hiện của hệ thống các giao tác sẽ thỏa mãn các công thức sau:

$$\varepsilon \cong \left(\bigwedge_{x \in \theta} [Wr_0(x)] \wedge \bigwedge_{i \leq n, x \in \theta} [\neg Vw_i(x)] \right) \wedge true \wedge [F].$$

Như vậy, một thời đoạn thỏa ε thì ở những thời điểm đầu mọi giao tác hoặc đọc hoặc ghi bất kỳ dữ liệu x nào đó và ở giai đoạn cuối thì mọi giao tác sẽ được ủy thác hoặc bị hủy bỏ.

Các tiên đề sau đề cập đến một số tính chất quan trọng của hệ thống các trạng thái và mối quan hệ của chúng.

Tiên đề 1. Nếu cần ghi dữ liệu thì tại mỗi thời điểm, chỉ có đúng một giao tác ghi dữ liệu (Wr) được thực hiện.

$$[\bigvee_{0 \leq i \leq n} Wr_i(x)], \quad (1)$$

$$[Wr_i(x)] \Rightarrow \bigwedge_{i \neq j} [\neg Wr_j(x)]. \quad (2)$$

Tiên đề 2. Với mọi giao tác T_i ($i \leq n$) và mọi đối tượng dữ liệu x , các trạng thái $Vw_i(x)$, cm_i và ab_i có thể thay đổi một lần, và trạng thái cm_i , ab_i là duy nhất.

$$[Vw_i(x)] \wedge true \Rightarrow [Vw_i(x)], \quad (3)$$

$$[cm_i] \wedge true \Rightarrow [cm_i], \quad (4)$$

$$[ab_i] \wedge true \Rightarrow [ab_i], \quad (5)$$

$$[cm_i] \Rightarrow [\neg ab_i]. \quad (6)$$

Tiên đề 3. Từ giả thiết của việc ủy thác nguyên tử, nếu một giao tác ghi một số đơn vị dữ liệu vào trong CSDL, thì nó sẽ được ủy thác tại thời điểm kết thúc.

$$\varepsilon \Rightarrow (\diamond [Wr_i(x)] \Rightarrow true \wedge [cm_i]). \quad (7)$$

Ký hiệu ENV là tập các công thức từ (1) đến (7).

4.2. Khả tuần tự của các giao tác

Hai phép toán được gọi là xung đột nếu chúng cùng thao tác trên cùng một đơn vị dữ liệu, trong đó có ít nhất một thao tác ghi (*write*). Như vậy việc thực hiện tương tranh của các giao tác là khả tuần tự nếu trên tập các giao tác đó xác định một quan hệ thứ tự tổng thể sao cho nếu giao tác T đứng trước T' thì mọi thao tác O của T phải thực hiện trước những thao tác O' của T' , xung đột với O để thực hiện tương tranh.

Thứ tự giữa các giao tác T_i và T_j , $i \neq j$ có xung đột trên đối tượng dữ liệu x được định nghĩa hình thức như sau:

$$WR_{ij}(x) \cong \diamond ([Wr_i(x)] \wedge [\neg Vw_j(x)]) \wedge true \wedge [Vw_j(x)],$$

$$RW_{ij}(x) \cong \diamond ([Vw_i(x)] \wedge [\neg Wr_j(x)]) \wedge true \wedge [Wr_j(x)],$$

$$WW_{ij}(x) \cong \diamond ([Wr_i(x)] \wedge true \wedge [Wr_j(x)]),$$

Vì vậy, $WR_{ij}(x)$ thực hiện trong khoảng thời gian nào đó nếu giá trị của x được ghi bởi giao tác T_i một số lần trong khoảng đó và sau đó các giao tác T_j thực hiện đọc trên x . Tương tự cho

những trường hợp khác.

Các ký hiệu RW_{ij} , WR_{ij} và WW_{ij} xác định thứ tự cần thực hiện của các giao tác T_i và T_j khi có xung đột trên một đơn vị dữ liệu nào đó.

$$RW_{ij} \cong \bigvee_{x \in \theta} RW_{ij}(x) \wedge TC_{ij},$$

$$WR_{ij} \cong \bigvee_{x \in \theta} WR_{ij}(x) \wedge TC_{ij},$$

$$WW_{ij} \cong \bigvee_{x \in \theta} WW_{ij}(x) \wedge TC_{ij},$$

ở đây $TC_{ij} \cong true \wedge [cm_i \wedge cm_j]$.

Quan hệ thứ tự giữa các giao tác có xung đột được định nghĩa như trên cho phép hệ thống thực hiện tuần tự hóa khi xử lý.

Tiếp theo chúng ta sử dụng C_{ij}^n mô tả quan hệ thứ tự thực hiện với mỗi $i, j, k, i \neq j \neq k$, được định nghĩa như sau:

$$C_{ij}^1 \cong RW_{ij} \vee WR_{ij} \vee WW_{ij},$$

$$C_{ij}^2 \cong C_{ij}^1 \vee (C_{ik}^1 \wedge C_{kj}^1),$$

...

$$C_{ij}^n \cong C_{ij}^{n-1} \vee (C_{ik}^{n-1} \wedge C_{kj}^{n-1}).$$

Từ đó chúng ta có:

Điều kiện khả tuần tự: Một thực hiện tương tranh của tập giao tác là khả tuần tự nếu nó thỏa mãn công thức nêu trên (C_{ij}^n) và thỏa công thức *SERIAL* cho mọi thời khoảng.

$$SERIAL \cong \varepsilon \Rightarrow \bigwedge_{i,j \leq n, i \neq j} \neg(C_{ij}^n \wedge C_{ji}^n).$$

4.3. Giao thức điều khiển tương tranh bằng khóa hai pha

Trong phần này chúng ta xét mô hình đặc tả hình thức 2PL-CCP [2]. Trong 2PL-CCP, mỗi đối tượng dữ liệu có một khóa đọc (read lock) và một khóa ghi (write lock). Một giao tác có thể thực hiện đọc (ghi) trên đối tượng dữ liệu x khi và chỉ khi nó giữ được khóa đọc (ghi tương ứng) trên x . Hai khóa được gọi là xung đột nếu chúng được gán cho cùng đối tượng dữ liệu và ít nhất một thao tác trong chúng là khóa ghi. Các giao tác chỉ có thể chia sẻ những khóa không xung đột, nghĩa là những khóa đọc. Để hình thức hóa giao thức, với mỗi $i \leq n, x \in \theta$, biến trạng thái $rl_i(x)$ và $wl_i(x)$ thể hiện khóa đọc (rl_i) hoặc khóa ghi (wl_i) trên x giữ một số lần bởi giao tác T_i hoặc không lần nào.

$$rl_i, wl_i \in \theta \rightarrow Time \rightarrow \{0, 1\},$$

$$rl_i(x)(t) = 1, \text{ nếu giao tác } T_i \text{ giữ khóa đọc trên } x \text{ tại thời điểm } t.$$

$$wl_i(x)(t) = 1, \text{ nếu giao tác } T_i \text{ giữ khóa ghi trên } x \text{ tại thời điểm } t.$$

Mọi giao tác có thể đều thực hiện theo hai pha. Trong pha đầu, đối tượng giữ khóa dữ liệu được thực hiện, trong khi pha thứ hai đối tượng khóa được giải phóng. Vì vậy, với mỗi giao tác T_i ta sử dụng một biến trạng thái ph_i thể hiện pha giao tác T_i trong cùng một thời điểm.

$$ph_i : Time \rightarrow \{0, 1\}, Ph_i(t) = 1, \text{ nếu giao tác } T_i \text{ trong pha nhận - pha đầu.}$$

Vì vậy, 2PL-CCP được hình thức hóa theo công thức DC như sau:

Khóa xung đột không thể chia sẻ được bởi các giao tác. Do đó, với mỗi $i, j \leq n, i \neq j, x \in \theta$

$$[rl_i(x)] \Rightarrow [\neg wl_j(x)], \quad (8)$$

$$[wl_i(x)] \Rightarrow [\neg rl_j(x)] \wedge [\neg wl_j(x)]. \quad (9)$$

Pha nhận luôn thực hiện trước pha giải phóng với mọi giao tác T_i

$$\varepsilon \Rightarrow [ph_i] \wedge [\neg ph_i]. \quad (10)$$

Một giao tác có thể ở trong pha nhận chỉ khi nó không ủy thác hoặc hủy bỏ

$$[ph_i] \Rightarrow [\neg cm_i] \wedge [\neg ab_i]. \quad (11)$$

Một giao tác có thể nhận các khóa chỉ khi nó đang là pha nhận. Vì vậy

$$[\neg rl_i(x)] \wedge [rl_i(x)] \Rightarrow [\neg rl_i(x)] \wedge [ph_i] \wedge true, \quad (12)$$

$$[\neg wl_i(x)] \wedge [wl_i(x)] \Rightarrow [\neg wl_i(x)] \wedge [ph_i] \wedge true. \quad (13)$$

Một giao tác có thể giải phóng một khóa trên đối tượng dữ liệu chỉ trong pha 2

$$[rl_i(x)] \wedge [\neg rl_i(x)] \Rightarrow [rl_i(x)] \wedge [\neg ph_i] \wedge true, \quad (14)$$

$$[wl_i(x)] \wedge [\neg wl_i(x)] \Rightarrow [wl_i(x)] \wedge [\neg ph_i] \wedge true. \quad (15)$$

Một giao tác có thể đọc hoặc ghi trên đối tượng dữ liệu chỉ khi nó giữ khóa tương ứng trên đối tượng dữ liệu ở cùng một thời điểm

$$[\neg V w_i(x)] \wedge [V w_i(x)] \Rightarrow \diamond [rl_i(x)], \quad (16)$$

$$[\neg W r_i(x)] \wedge [W r_i(x)] \Rightarrow \diamond [wl_i(x)]. \quad (17)$$

Kí hiệu $2PLC$ là tập các công thức DC từ (8) tới (17) và $TWOPHASE \cong \bigwedge_{\varphi \in 2PLC} \square \varphi$. Từ đó

chúng ta có

Định lý 1. *SERIAL* là dẫn được từ *ENV* và $2PLC$, nghĩa là
 $ENV, 2PLC \vdash SERIAL$.

Theo định lý suy dẫn thì $TWOPHASE \Rightarrow SERIAL$ dưới *ENV*, do vậy tất cả các thực hiện của hệ thống giao tác tạo ra bởi $2PLC$ -CCP đều là khả tuần tự.

Để chứng minh được định lý trên chúng ta cần các bổ đề sau:

Bổ đề 1. Với $2PLC$, cho $i \leq n$

$$\varepsilon \Rightarrow \square (true \wedge [ph_i] \Rightarrow [ph_i]),$$

$$\varepsilon \Rightarrow \square ([\neg ph_i] \wedge true \Rightarrow [\neg ph_i]).$$

Chứng minh:

$$\varepsilon \Rightarrow [ph_i] \wedge [\neg ph_i] \quad (10)$$

$$\Rightarrow \square [ph_i]^* \wedge \square [\neg ph_i]^* \quad (DC-9)$$

$$\Rightarrow \square ([ph_i]^* \vee [\neg ph_i]^* \vee [ph_i]^* \wedge [\neg ph_i]^*) \quad (DC-18)$$

$$\Rightarrow \square (true \wedge [ph_i] \Rightarrow [ph_i])^* \quad (DC-1), (DC-4), PC$$

Bổ đề 2. Cho $i, j \leq n, i \neq j$

$$2PLC \vdash \varepsilon \wedge \diamond [\neg ph_i] \wedge [ph_j] \Rightarrow ([ph_i] \wedge [ph_j]) \wedge ([\neg ph_i] \wedge [ph_j]) \wedge ([\neg ph_i] \wedge [\neg ph_j]).$$

Chứng minh:

$$\varepsilon \wedge \diamond [\neg ph_i] \wedge [ph_j] \quad (10), PL$$

$$\Rightarrow ([ph_i] \wedge [\neg ph_i] \wedge [ph_j] \wedge [\neg ph_j] \wedge \diamond [\neg ph_i] \wedge [ph_j]) \quad (DC-1), Def DC$$

$$\Rightarrow ([ph_i] \wedge true \wedge true \wedge [\neg ph_j] \wedge true \wedge [\neg ph_i] \wedge [ph_j] \wedge true) \quad (DC-13)$$

$$\Rightarrow (true \wedge [\neg ph_j] \wedge [ph_i] \wedge true \wedge [\neg ph_i] \wedge [ph_j] \wedge true) \quad (DC-12), (DC-1)$$

$$\Rightarrow (true \wedge [\neg ph_j] \wedge true \wedge [ph_i] \wedge [\neg ph_i] \wedge [ph_j] \wedge true) \quad B1, (DC-1)$$

$$\Rightarrow ([ph_i] \wedge [\neg ph_i] \wedge [ph_j] \wedge true \wedge [ph_j]) \quad (DC-14)$$

$$\Rightarrow ([ph_i] \wedge [\neg ph_i] \wedge [ph_j] \wedge [ph_j] \wedge true) \quad (DC-12) (DC-1)$$

$$\Rightarrow ([ph_i] \wedge [\neg ph_i] \wedge [ph_j] \wedge [\neg ph_j]) \quad B1, (DC-1)$$

$$\Rightarrow [ph_i] \wedge ([\neg ph_i] \wedge true \wedge true \wedge [ph_j]) \wedge [\neg ph_j] \quad PL, (DC-1)$$

$$\Rightarrow [ph_i] \wedge ([\neg ph_i] \wedge [ph_j]) \wedge [\neg ph_j] \quad B1, (DC-1)$$

$$\Rightarrow (true \wedge [ph_j] \wedge [ph_i] \wedge ([\neg ph_i] \wedge [ph_j])) \wedge [\neg ph_j] \quad PL, (DC-1)$$

$$\Rightarrow ([ph_i] \wedge [ph_j]) \wedge ([\neg ph_i] \wedge [ph_j]) \wedge [\neg ph_j] \quad B1, (DC-15)$$

$$\begin{aligned} &\Rightarrow ([ph_i] \wedge [ph_j]) \wedge (true \wedge [\neg ph_i] \wedge ([\neg ph_i] \wedge [ph_j]) \wedge [\neg ph_j]) && \text{PL, (DC-1)} \\ &\Rightarrow ([ph_i] \wedge [ph_j]) \wedge ([\neg ph_i] \wedge [ph_j]) \wedge ([\neg ph_i] \wedge [\neg ph_j]) && \text{B1, (DC-15)} \end{aligned}$$

Bổ đề 3. Cho $m, i, j \leq n, i \neq j$

$$ENV, 2PLC \vdash \varepsilon \wedge C_{ij}^m \Rightarrow \diamond[\neg ph_i] \wedge [ph_j].$$

Chứng minh: Với $i, j \leq n, i \neq j$, ta có

$$\begin{aligned} &\varepsilon \wedge RW_{ij} \\ &\Rightarrow ([\neg Vw_i(x)] \wedge true \wedge \diamond[Vw_i(x) \wedge \neg Wr_j(x)] \wedge true \wedge [Wr_j(x)]) && \text{def } \varepsilon, RW_{ij}, \text{ (DC-1)} \\ &\Rightarrow ([\neg Vw_i(x)] \wedge true \wedge \diamond[Vw_i(x)] \wedge [\neg Wr_j(x)] \wedge true \wedge [Wr_j(x)]) && \text{(DC-8), (DC-10), (DC-1)} \\ &\Rightarrow ([Vw_i(x)] \wedge [\neg Vw_i(x)] \wedge true \wedge [Wr_j(x)] \wedge [\neg Wr_j(x)]) && \text{(DC-12), (DC-13), (DC-1)} \\ &\Rightarrow \diamond[rl_i(x)] \wedge true \wedge \diamond[wl_j(x)] && \text{(16), (17), (DC-1)} \\ &\Rightarrow \diamond[rl_i(x)] \wedge [\neg wl_j(x)] \wedge true \wedge [wl_j(x)] && \text{(8), (DC-8), (DC-1)} \\ &\Rightarrow \diamond[rl_i(x)] \wedge true \wedge [wl_j(x)] \wedge [\neg wl_j(x)] && \text{(DC-12), (DC-1)} \\ &\Rightarrow \diamond[rl_i(x)] \wedge true \wedge [wl_j(x) \wedge ph_j] && \text{(13), (DC-1), (DC-8)} \\ &\Rightarrow \diamond[rl_i(x)] \wedge true \wedge [\neg rl_i(x)] \wedge [ph_j] && \text{(9), PL, (DC-8), (DC-1)} \\ &\Rightarrow \diamond[rl_i(x)] \wedge [\neg rl_i(x)] \wedge true \wedge [ph_j] && \text{(DC-12), (DC-1)} \\ &\Rightarrow \diamond[\neg ph_i] \wedge true \wedge [ph_j] && \text{(14), (DC-1), (DC-8)} \\ &\Rightarrow \diamond[\neg ph_i] \wedge [ph_j] && \text{B1, (DC-1)} \end{aligned}$$

$$\begin{aligned} \varepsilon \wedge RW_{ij} &\Leftrightarrow \varepsilon \wedge \bigvee_{x \in \theta} RW_{ij}(x) \wedge TC_{ij} \\ &\Leftrightarrow \bigvee_{x \in \theta} (\varepsilon \wedge RW_{ij}(x) \wedge TC_{ij}) && \text{PL} \\ &\Rightarrow \diamond[\neg ph_i] \wedge [ph_j]. \end{aligned}$$

Chứng minh tương tự chúng ta cũng thể có thể thiết lập được

$$\begin{aligned} \varepsilon \wedge WR_{ij}(x) &\Rightarrow \diamond[\neg ph_i] \wedge [ph_j], \\ \varepsilon \wedge WW_{ij}(x) &\Rightarrow \diamond[\neg ph_i] \wedge [ph_j]. \end{aligned}$$

Bây giờ chúng ta chứng minh bổ đề dựa trên qui nạp trên m :

Xét bước qui nạp cơ sở:

$$\begin{aligned} \varepsilon \wedge C_{ij}^1 &\Leftrightarrow \varepsilon \wedge (RW_{ij} \vee WR_{ij} \vee WW_{ij}) && \text{Def } C_{ij}^1 \\ &\Leftrightarrow (\varepsilon \wedge RW_{ij}) \vee (\varepsilon \wedge WR_{ij}) \vee (\varepsilon \wedge WW_{ij}) && \text{PL} \\ &\Rightarrow \diamond[\neg ph_i] \wedge [ph_j]. \end{aligned}$$

Qui nạp thừa nhận: (IA)

$$\varepsilon \wedge C_{ij}^t \Rightarrow \diamond[\neg ph_i] \wedge [ph_j].$$

Bước qui nạp tiếp: (IS)

Chúng ta chứng minh rằng với $i, j, k \leq n, i \neq j \neq k$

$$\varepsilon \wedge C_{ik}^t \wedge C_{kj}^t \Rightarrow \diamond[\neg ph_i] \wedge [ph_j].$$

Thật vậy

$$\begin{aligned} \varepsilon \wedge C_{ik}^t \wedge C_{kj}^t &\Rightarrow \varepsilon \wedge \diamond[\neg ph_i] \wedge [ph_k] \wedge \diamond[\neg ph_k] \wedge [ph_j] && \text{(IA)} \\ &\Rightarrow [ph_k] \wedge ([\neg ph_k] \wedge [\neg ph_i]) \wedge [ph_k] \wedge ([\neg ph_k] \wedge [ph_j] \wedge [\neg ph_j]) && \text{B2, PL, (DC-1)} \\ &\Rightarrow [ph_k] \wedge ([\neg ph_k] \wedge [\neg ph_i]) \wedge [ph_j] \wedge [\neg ph_j] && \text{(DC-16)} \\ &\Rightarrow true \wedge [\neg ph_i] \wedge [ph_j] \wedge [\neg ph_i] \wedge [\neg ph_j] && \text{(DC-15), PL, (DC-1)} \\ &\Rightarrow true \wedge [\neg ph_i] \wedge [ph_j] \wedge true && \text{PL, (DC-1)} \\ &\Rightarrow \diamond[\neg ph_i] \wedge [ph_j] && \text{(DC-8)} \end{aligned}$$

$$\begin{aligned}
\varepsilon \wedge C_{ij}^{t+1} &\Rightarrow \varepsilon \wedge (C_{ij}^t \vee (C_{ik}^t \wedge C_{kj}^t)) && \text{Def } C_{ij}^{t+1} \\
&\Rightarrow (\varepsilon \wedge C_{ij}^t) \vee (\varepsilon \wedge C_{ik}^t \wedge C_{kj}^t) && \text{PL} \\
&\Rightarrow \diamond[\neg ph_i]^\cap [ph_j]. && \text{IA, IS, PL}
\end{aligned}$$

Chứng minh Định lý 1:

Từ các bổ đề trên ta suy ra: Với $i, j \leq n, i \neq j$,

$$\begin{aligned}
\varepsilon \wedge C_{ij}^n \wedge C_{ji}^n &\Rightarrow \varepsilon \wedge \diamond[\neg ph_i]^\cap [ph_j] \wedge \diamond[\neg ph_j]^\cap [ph_i] && \text{B3, PL} \\
&\Rightarrow ([ph_j]^\cap ([\neg ph_j] \wedge [\neg ph_i]) \wedge [ph_j]^\cap ([\neg ph_j] \wedge [ph_i]^\cap [\neg ph_i])) && \text{B2, PL, (DC-15), (DC-1)} \\
&\Rightarrow [ph_j]^\cap ([\neg ph_j] \wedge [\neg ph_i] \wedge [ph_i]^\cap [\neg ph_i]) && \text{(DC-16)} \\
&\Rightarrow [ph_j]^\cap \text{false} && \text{(DC-15), PL, (DC-1), (DC-4)} \\
&\Rightarrow \text{false} && \text{(DC-4)} \\
\Leftrightarrow \varepsilon &\Rightarrow \bigwedge_{i,j \leq n, i \neq j} \neg(C_{ij}^n \wedge C_{ji}^n).
\end{aligned}$$

Như vậy ta có: $ENV, 2PLC \vdash SERIAL$. Định lý đã được chứng minh.

5. KẾT LUẬN

Với logic DC chúng ta có thể đặc tả được những hệ thống lớn, phức tạp như hệ CSDLTGT. Vấn đề chính trong bài báo là đặc tả hình thức giao thức điều khiển tương tranh khóa hai pha trong logic DC. Kết quả chứng minh tính khả tuần tự của 2PL-CCP khẳng định được tính đúng của hệ thống các giao tác đảm bảo được tính nhất quán dữ liệu trong CSDLTGT.

TÀI LIỆU THAM KHẢO

- [1] A. Bestavros, J. Lin, and Sany Hyuk Son, *Real Time Database System: Issue and Application*, Kluwer Academic publishers, 1997.
- [2] Đoàn Văn Ban, Hồ Văn Hương, Đặc tả hình thức điều khiển tương tranh trong cơ sở dữ liệu thời gian thực, *Proceedings of Institute of Information Technology, Conference at Hue University*, 6 - 2000.
- [3] Đoàn Văn Ban, Hồ Văn Hương, "A Formal Verification of the Concurrency Control in Duration Calculus", Conference at Institute of Mathematics, 8 - 2000.
- [4] Đoàn Văn Ban, Hồ Văn Hương, "Tính nhất quán lâm thời trong cơ sở dữ liệu thời gian thực", Xemina tháng 10 - 2000, Trường Đại học Khoa học tự nhiên, ĐHQG Hà Nội.
- [5] Đoàn Văn Ban, Hồ Văn Hương, "Duration Calculus and Application", Conference of Mathematics, Mechanics, Informatics, 2000, Hanoi University of Sciences, National University.
- [6] Đặng Văn Hưng, *Modelling and Verification of Biphase Mark Protocols Using PVS/DC*, UNU/IIST Report No. 103, April, 1997.
- [7] Ekaterina Pavlova, Đặng Văn Hưng, *A formal Specification of the Concurrency Control in Real Time Database*, UNU/IIST Report No. 152, January, 1999.
- [8] J. Stankovic et al., Misconceptions about real time databases, *IEEE Computer* (1999).
- [9] Jeffrey D. Ullman, *Principles of Database and Knowledge Base System*, Prentice Hall, 1987.
- [10] M.R. Hasnen, Zhou Chao Chen, A. P. Ravn, Duration calculus: Logical foundations, *Formal Aspects of Computing* (1997).
- [11] P. X. Novikov, người dịch: Nguyễn Hữu Ngự, Đặng Huy Nhuận, *Đại cương Logic Toán*, NXB Khoa học Kỹ thuật, Hà Nội, 1971.

Nhận bài ngày 5 tháng 1 năm 2001

Nhận bài sau khi sửa ngày 24 tháng 5 năm 2001

Đoàn Văn Ban - Viện Công nghệ thông tin.
 Hồ Văn Hương - Ban Cơ yếu Chính phủ.