

Il controllo della concorrenza

di Anna Pugliese

seconda puntata

Il problema del Controllo della Concorrenza, presentato sul precedente numero di MC, nasce con l'uso del parallelismo fra diverse attività in esecuzione su un sistema che utilizzano risorse comuni alle attività stesse. Two phases locking e Timestamping sono i nomi dei due più classici meccanismi di controllo della concorrenza realmente utilizzati dai computer attualmente in commercio. Il primo di essi verrà presentato in questo numero della rubrica, il secondo assieme agli ultimi sviluppi della ricerca in materia, saranno oggetto di una successiva ed ultima parte dedicata a questo tema. L'articolo comprende la presentazione di alcuni problemi strettamente legati al controllo della concorrenza, fra i quali il famoso deadlock

Una precisa visione del problema

È doveroso richiamare alcuni punti trattati il mese scorso. Primo fra tutti, l'individuazione degli attori: Transazioni e Risorse.

La transazione è un costrutto di programmazione mediante il quale è possibile racchiudere una generica sequenza di operazioni, ognuna delle quali può o meno agire su di un dato condiviso, in una specie di unica, grande operazione.

Un importante aspetto delle transazioni è il loro punto di commit. Per chiarire questo concetto occorre tener conto del fatto che le transazioni sono uno strumento mediante il quale è possibile trattare sia il problema del controllo della concorrenza che quello della tolleranza ai guasti dei sistemi di elaborazione. Dal punto di vista della concorrenza, una transazione è una quantità indivisibile d'elaborazione, l'effetto della sua esecuzione deve coincidere con quello che si sarebbe ottenuto eseguendo la transazione in assenza di concorrenza. Dal punto di vista dell'affidabilità, una transazione è una quantità indivisibile d'elaborazione il cui effetto, anche in presenza di guasti, dev'essere o nullo oppure identico a quello di una corretta esecuzione dell'intera transazione. Guardando le cose in maniera integrata, l'esecuzione di una transazione corrisponderà all'esecuzione di tutte le operazioni, di cui essa è composta, non sui dati effettivi ma su copie dei dati stessi. In seguito all'esecuzione dell'ultima operazione verrà poi inserita un'operazione di commit, il cui scopo è quello di convalidare gli effetti della transazione. Tale convalida avviene solo nel caso in cui non si sono verificati errori e non si sono create inconsistenze sui dati per effetto di un'errata serializzazione, in tal caso la transazione viene COMMITTATA, altrimenti viene ABORTITA. Sul sistema per la gestione della base di dati, in un generico istante, saranno in esecuzione un certo numero di transazioni concorrenti molte delle quali si troveranno ad agire su archivi comuni. Tali archivi saranno allora considerati come risorse condivise dalle transazioni.

Considerando il succedersi degli

eventi dal punto di vista di una precisa risorsa, è facile comprendere che le modifiche apportate al suo valore non possono essere considerate assolute, ma relative alla transazione che ha generato la modifica. Le operazioni sulle risorse saranno allora considerate come coppie (op, tid), dove op (OPERation) specifica il tipo di operazione invocata sulla risorsa e tid (Transaction IDentifier) l'identificatore associato alla transazione richiedente.

Ora, ogni operazione su un dato condiviso è di per sé un'operazione critica; essa va eseguita con particolari accorgimenti quali ad esempio il locking del dato condiviso durante l'operazione. Il locking di un dato è un'operazione di privatizzazione temporanea della struttura contenente il dato stesso. Essa viene implementata associando ad ogni dato condiviso una chiave (to lock = chiudere a chiave) dal cui valore è possibile capire se il dato è stato o meno privatizzato temporaneamente da qualche transazione. Tutto ciò ha lo scopo di impedire l'esecuzione contemporanea di operazioni diverse sullo stesso oggetto. Il lettore interessato ad una più approfondita trattazione di questo argomento è rimandato a questa stessa rubrica pubblicata sul numero 52 di MC.

Data per scontata l'adozione di opportuni meccanismi che garantiscano che in un certo istante su un certo oggetto esiste al più una operazione in esecuzione, lo scopo da prefiggersi è quello di permettere che su un certo oggetto in un certo istante sia possibile mantenere in esecuzione tutte le transazioni che si vuole, vale a dire eseguire in sequenza operazioni appartenenti a transazioni diverse. Tutto questo, a condizione di mantenere l'integrità dell'oggetto stesso.

L'esecuzione seriale

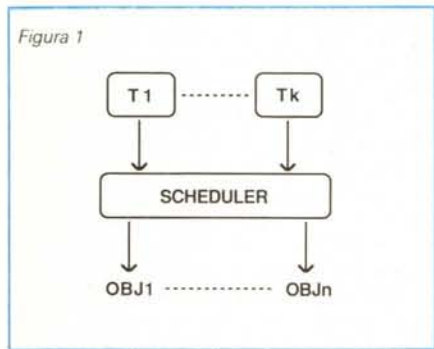
Dato un certo numero di transazioni, il più semplice metodo per eseguirle senza problemi è quello di utilizzare uno scheduling seriale. Con riferimento alla figura 1, basterà implementare un processo scheduler (ordinatore) al quale tutte le transazioni dovranno essere indirizzate per essere da esso stesso eseguite, se-

rialmente, mediante l'invocazione delle operazioni, specificate in ogni transazione, all'oggetto corrispondente. È evidente che tale processo costituisce un collo di bottiglia per il sistema, e che il parallelismo nell'esecuzione delle transazioni è, in tal caso, perso.

Il locking a due fasi

Il locking a due fasi, anche conosciuto con la sigla 2PL che sta per Two Phases Locking, è un meccanismo per il controllo della concorrenza molto particolare, oltre ad essere il più diffuso fra quelli esistenti. La sua peculiarità risiede nel fatto che esso è un meccanismo statico, vale a dire che la sua funzionalità è dovuta al modo in cui la transazione è strutturata.

Esso è basato sul requisito, cui ogni transazione deve soddisfare, di suddivi-



dere la transazione in due fasi: la growing phase (fase crescente) e la shrinking phase (fase decrescente). Durante la prima fase, la transazione può richiedere tutti i lock di cui necessita per svolgere le sue operazioni ogni volta che un'operazione su un nuovo oggetto viene generata.

Tali lock devono essere trattenuti fino a quando la transazione raggiunge il suo punto di commit, a questo punto ha inizio la seconda fase della transazione consistente nel rilascio di tutti i lock precedentemente richiesti.

Il parallelismo esplicitato con l'uso di questo meccanismo di controllo della concorrenza dipende dalle collisioni fra le richieste di lock sugli oggetti avanzate da parte delle varie transazioni. Se su un certo oggetto è in esecuzione un'operazione di una transazione, tale oggetto non potrà essere acceduto da nessun'altra transazione fino al completamento della transazione che ne possiede il lock.

Se ne ricava che non esiste parallelismo sugli oggetti. Al più saranno eseguibili in parallelo transazioni operanti su insiemi di oggetti disgiunti.

2PL con prerilascio

Una variante del metodo 2PL è la cosiddetta versione con prerilascio. Essa è basata sulla possibilità di rilasciare i lock posseduti dalla transazione prima ancora di giungere al punto di commit, non appena l'oggetto del quale si intende prerilasciare il lock non è più necessario alla transazione stessa, ma a condizione che in seguito al rilascio di un qualsiasi lock non vengano richiesti lock su nessun altro oggetto. Quest'ultima condizione è necessaria per garantire la strutturazione a due fasi della transazione, senza la quale l'esecuzione potrebbe generare inconsistenze nei dati.

Riguardiamo l'esempio

Entrambe le versioni del locking a due fasi sono pensate per operare con transazioni che coinvolgono un qualunque numero di operazioni su un qualunque numero di oggetti. Nondimeno può essere utile vederne l'applicazione su un caso molto semplice qual è quello presentato la volta scorsa. La procedura è riportata in figura 2, essa ha lo scopo di prenotare un posto sul volo specificato dal parametro flight per il giorno indicato da day, FREE(i,j) è l'elemento della matrice bidimensionale, che costituisce la risorsa condivisa, indicante il numero dei posti ancora disponibili sul volo i per il giorno j.

In figura 3 sono riportate le due pro-

```

procedure PRENOTATION ( flight, day );
begin
N := FREE ( flight, day );
if N > 0 then
    begin
    FREE ( flight, day ) := N-1;
    Result := "done"
    end
    else
    Result := "not done"
end;
    
```

Figura 2. La procedura di prenotazione vista il mese scorso, che attivata due volte concorrentemente causa inconsistenze sui dati.

cedure scritte in accordo ai due meccanismi di controllo della concorrenza precedentemente illustrati.

Gli aborti in cascata

Potrebbe, a prima vista, sembrare ovvia la convenienza ad utilizzare la versione del 2PL con prerilascio rispetto a quella base. Tuttavia essa presenta un inconveniente molto sottile, ma che in ambienti in cui l'uso del parallelismo fra le transazioni è massiccio, potrebbe degradare la performance del sistema a livelli inaccettabili. Si consideri a tal proposito e nel caso in cui il meccanismo di controllo della concorrenza utilizzato è il 2PL con prerilascio, una transazione T1 che dopo aver prerilasciato un certo numero di lock su oggetti da essa modificati nel corso della sua esecuzione, venga abortita a causa, si supponga, di un errore. Ciò renderà necessario abortire anche eventuali altre transazioni che avevano acquisito il lock prerilasciato da T1, essendo la correttezza della loro esecuzione subordinata al buon esito della transazione abortita. Se si considera la possibilità che queste nuove transazioni da abortire, prima ancora che vengano effettivamente abortite, abbiano modificato e prerilasciato oggetti condivisi, si comprende facilmente come questo possa dar vita ad una serie di aborti, detti appunto in cascata, dagli effetti certamente disastrosi dal punto di vista dell'efficienza.

```

-----
procedure PRENOTATION ( flight, day );
-----
begin
LOCK (FREE(flight,day));
N := FREE(flight,day );
if N > 0
then
begin
FREE(flight,day) := N-1;
Result := "done"
end
else
Result := "not done";
UNLOCK (FREE(flight,day))
end;
-----
(a)
-----
:: begin
:: LOCK (FREE(flight,day));
:: N := FREE(flight,day);
:: if N > 0
:: then
:: begin
:: FREE(flight,day) := N-1;
:: UNLOCK (FREE(flight,day));
:: Result := "done"
:: end
:: else
:: Result := "not done"
:: end;
-----
(b)
-----
    
```

Figura 3 - La procedura illustrata in figura 2 scritta in accordo al metodo Two Phases Locking, rispettivamente in versione base (fig. 3a) ed in versione con prerilascio (fig. 3b).

Ta::	lock (X)	t1 :	Tb::	lock (W)
	(opX,ta)	t2 :		(opW,tb)
	lock (Y)	t3 :		lock (Z)
	(opY,ta)	t4 :		(opZ,tb)
	lock (Z)	t5 :		lock (Y)
	unlock (X)	t6 :		unlock (W)
	(opZ,ta)	t7 :		(opY,tb)
	unlock (Z)	t8 :		unlock (Y)
	(opY,ta)	t9 :		(opZ,tb)
	unlock (Y)	t10 :		unlock (Z)
	COMMIT	t11 :		COMMIT

Figura 4.
Due transazioni agenti sugli oggetti X, Y, Z, e W. L'espressione (opX,ta) designa una qualsiasi operazione invocata dalla transazione ta sull'oggetto X. Le due transazioni sono strutturate in accordo al meccanismo di controllo della concorrenza 2PL con prerilascio. Si noti la strutturazione a due fasi delle transazioni: da t1 a t5 GROWING PHASE e da t6 a t11 SHRINKING PHASE.

Deadlock

Consideriamo ora le due transazioni descritte in figura 4. Esse sono strutturate in accordo al meccanismo di locking a due fasi in versione con prerilascio, ma quanto detto nel seguito vale anche nel caso della versione 2PL con ritenzione fino al commit.

Per non appesantire troppo la descrizione, si assuma che la durata di tutte le operazioni sia fissa e che nel generico istante T_i ($1 \leq i \leq 11$), come indicato in figura, vengano eseguite in parallelismo reale le i -esime operazioni di Ta e Tb.

Fino all'istante t4 le prime due operazioni di Ta e le prime due operazioni di Tb saranno eseguite senza problemi, essendo operazioni su oggetti distinti.

Nell'istante t5 la transazione Ta richiederà il lock sull'oggetto Z prima di poter procedere nell'esecuzione della sua terza operazione. Tale lock non potrà essere ottenuto da Ta in quanto già assegnato, fin dall'istante t3, alla transazione Tb che lo tratterrà fino a t10, a motivo della necessità di riutilizzare l'oggetto Z nell'istante t9. La transazione Ta verrà dunque sospesa in attesa che tale lock venga rilasciato. Purtroppo ciò non avverrà mai in quanto la transazione Tb, nello stesso istante verrà a trovarsi in un'altra situazione in attesa del lock sull'oggetto Y posseduto dalla transazione sospesa Ta.

La situazione che si è venuta a verificare nell'esempio descritto, prende il significativo nome di DEADLOCK (chiusura della morte). In effetti le due transazioni resteranno per sempre bloccate in attesa dei rispettivi lock, a meno che non si intervenga dall'esterno per sbloccare la situazione.

L'esempio presentato rispecchia uno dei modi più semplici in cui il deadlock può verificarsi, essendo solo due le transazioni coinvolte. In realtà non esiste un limite al numero di transazioni che possono rimanere coinvolte in simili situazioni di stallo. Il fenomeno del deadlock è comune a tutti i meccanismi di controllo della concorrenza, paradossalmente anche a quelli non basati sul lock esplicito degli oggetti. Per difendersi da questo fenomeno esistono due possibili:

lità: la prevenzione e la rilevazione del deadlock.

La prevenzione del deadlock consiste nell'utilizzare meccanismi capaci di impedire il verificarsi del fenomeno. Un simile meccanismo, anche se in forma del tutto implicita, è utilizzato dal metodo di controllo della concorrenza basato sui timestamp. Per ciò che riguarda il 2PL invece, i tentativi di utilizzare prevenzione del deadlock hanno spesso avuto esiti insoddisfacenti. A mo' di

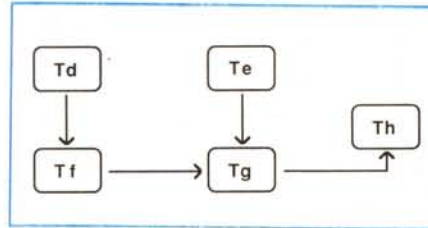


Figura 5 - Un esempio di wait-for graph.

cronaca tuttavia, si noti che un semplicissimo modo per farlo consiste nell'imporre il requisito di richiedere tutti i lock necessari all'inizio della transazione; se sono stati ottenuti tutti allora si procede, diversamente si rilasciano anche i pochi lock acquisiti e, dopo un certo intervallo di tempo, si ritenta l'acquisizione.

Più diffusa è invece l'utilizzazione di meccanismi di rilevazione del deadlock. Fra di essi, il più elegante consiste nella costruzione dei cosiddetti «WAIT-FOR GRAPHS» vale a dire grafi di precedenza (letteralmente: attesa per). In tali grafi, i nodi corrispondono alle transazioni, mentre gli archi diretti da una transazione in attesa ad un'altra in possesso del lock per cui la prima attende, esprimono proprio la condizione dei wait-for.

Un semplice modo per implementarli, è quello di affidarne l'aggiornamento alle stesse transazioni, nel momento in cui esse, eseguendo la primitiva di lock su un dato oggetto trovano l'oggetto stesso occupato da un'altra transazione. In tal caso la transazione che ha trovato l'oggetto occupato, prima di sospendersi, aggiornerà il grafo di precedenza, che potrebbe anche essere vuoto, aggiungendo ad esso un nodo che porta il

suo nome, un altro nodo che porta il nome della transazione in possesso del lock cercato, sempre che tali nodi non esistano già, ed un arco che va dal suo nodo a quello dell'altra. Infine, la transazione stessa effettuerà un controllo sul grafo così ottenuto. Se in tale grafo esiste un ciclo, il deadlock è stato rilevato. Basterà a questo punto forzare l'aborto di una delle transazioni coinvolte nel ciclo, in accordo a qualche predefinita politica.

Con riferimento alla figura 5, si supponga che quello in essa riportato sia l'attuale grafo di precedenza. Sul sistema saranno in esecuzione concorrente un numero di transazioni maggiore o uguale al numero dei nodi presenti sul grafo. Se a questo punto, la transazione Th, in possesso di un lock voluto anche da Tg, si sospende in attesa di un lock posseduto da Te, essa dovrà aggiornare il grafo con un arco direzionato da Th a Te, la qual cosa provocherà l'insorgere di un ciclo nel grafo stesso, a testimonianza dei verificarsi del deadlock. Si noti che il deadlock non coinvolge solo le transazioni nel ciclo, ma anche Td e Tf che attendono per Tg.

Per quanto riguarda il deadlock illustrato in figura 4, la semplicità della sua dinamica è testimoniata dal grafo di precedenza, illustrato in figura 6, che si sarebbe venuto a formare in tal caso.

Un simile meccanismo di rilevazione del deadlock è certamente assai elegante, come già accennato sopra, ma sicuramente dispendioso. L'aggiornamento del grafo da parte delle transazioni, ma ancor più il test di ciclicità potrebbero far trascorrere più tempo di quanto sarebbe necessario per avere il lock dispo-

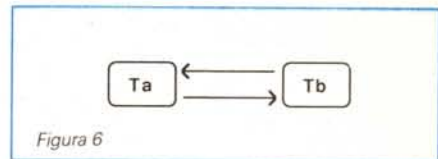


Figura 6

nibile. L'alternativa più diffusa, ai grafi di precedenza, consiste nell'uso di timeout: se una transazione attende per un tempo maggiore di una soglia definita a priori, decide di abortire se stessa per sbloccare un'eventuale situazione di deadlock. L'uso di timeout è diffuso un po' in tutte le aree di produzione del software, ma il problema di definire in maniera ottima la soglia di tempo di un timeout, oramai diventato storico nel campo dell'informatica, non è mai stato risolto brillantemente. Che un timeout alla fine, sia più o meno efficiente di un wait-for graph, è solo questione di fortuna.

