Adatbázisok elmélete 20. előadás

Katona Gyula Y.
Budapesti Műszaki és Gazdaságtudományi Egyetem
Számítástudományi Tsz.
I. B. 137/b
kiskat@cs.bme.hu
http://www.cs.bme.hu/˜kiskat

2005

Tranzakciókezelés

Eddig hallgatólagosan feltettük, hogy

- egy felhasználó van csak
- a lekérdezések/módosítások hiba nélkül lefutnak

A valóságban ez nincs így, két nagyobb gond is lehet, aminek kezelése a tranzakciókezelő dolga:

- **Többfelhasználós működés**: egyidejű hozzáférést kell biztosítani több felhasználónak, de úgy, hogy az adatbázis konzisztens maradjon (pl. banki rendszerek, helyfoglalás)
- **Rendszerhibák utáni helyreállítás**: ha a külső tár megmarad, de a belső sérül (vagy egyszerűen csak nem fut le valami) és emiatt az adatbázis inkonzisztens állapotba kerül, akkor újra konzisztens állapotba kell hozni (vagy visszacsinálni valamit, vagy befejezni valamit)

Ez két (néha egymással is ellentétes) kívánság, de az alapeszköz ugyanaz lesz: a **tranzakció**.

Megoldandó problémák

Többfelhasználós működés

A lekérdezésfeldolgozó a magas szintű utasításokból álló lekérdezéseket/módosításokat elemi utasításokra bontja, (pl: olvass ki valahonnan valamit, írj be valahova valamit, számolj valamit). Egy felhasználó egy lekérdezése/módosítása ilyen elemi utasítások sorozatává alakul.

1. felhasználó: $u_1, u_2, \ldots, u_{10}$
2. felhasználó: $v_1, v_2, \ldots, v_{103}$

De ez a két utasítássorozat nem elkülönülve jön, hanem összefésülődnek:

$$u_1, v_1, v_2, u_2, u_3, v_3, \ldots, v_{103}, u_{10}$$

A saját sorrend megmarad mindkettőn belül, de amúgy össze vannak keveredve, így lesz lehetséges a több felhasználó egyidejű kiszolgálása. Ebből viszont baj származhat, mert olyan állapot is kialakulhat, ami nem jött volna létre, ha egymás után futnak le a tranzakciók.

Példa

1. felhasználó: READ A, $A++$, WRITE A
2. felhasználó: READ A, $A++$, WRITE A

Ha ezek úgy fésülődnek össze, hogy

$$(\text{READ } A)_1, (\text{READ } A)_2, (A++)_1, (A++)_2, (\text{WRITE } A)_1, (\text{WRITE } A)_2$$

akkor a végén csak eggyel nő A értéke, holott kettővel kellett volna.

Rendszerhibák

Ha rendszerhiba van (a belső memória meghibásodik) vagy csak ABORT van (a tranzakciókezelő ütemező része kilő egy alkalmazást futás közben), akkor emiatt félbemaradhat valami, aminek nem lenne szabad.

Példa: átutalunk egyik helyről a másik helyre pénzt:

$$A := A - 50 \quad B := B + 50$$

Ha az a közepén meghal: hibás állapot jön létre.

Tranzakció

Alapfogalom mindkét problémakör megoldásában a **tranzakció**: egy felhasználóhoz tartozó elemi utasítások olyan sorozata, melynek fő jellemzője az **atomiság** (**A**tomicity): vagy az összes utasításnak végre kell hajtódnia vagy egynek sem szabad. Ez lesz az egyik dolog, amit mindenáron el akarunk majd érni.

További elvárások:

- **konzisztencia**, **C**onsistency: az adatbázis konzisztens állapotok között mozog, (hogy mit jelent a konzisztens, az a valóságtól függ, pl. banki összegek stimmelése), nem konzisztens állapot csak ideiglenesen állhat fenn (a rendszerhibák utáni helyreállításnál lesz ez fontos)
- **elkülönítés**, **I**solation: több tranzakció egyidejű futása után úgy kell kinéznie az adatbázisnak, mintha a tranzakciók nem lettek volna összefésülve (az ütemező dolga lesz ennek biztosítása)
- **tartósság**, **D**urability: a befejezett tranzakciók hatása nem veszhet el

Többfelhasználós működés, alapfogalmak

Cél: párhuzamos hozzáférés biztosítása, de úgy, hogy a konzisztencia megmaradjon

Feltételezzük, hogy ha a tranzakciók egymás után, elkülönítve futnak, akkor konzisztens állapotból konzisztens állapotba jut a rendszer. Csak azokat az összefésülődéseit akarjuk megengedni a tranzakcióknak, amelyeknek a hatása ekvivalens valamelyik izolálttal.

ütemezés: egy vagy több tranzakció műveleteinek valamilyen sorozata (fontos, hogy a tranzakciókon belüli sorrend megmarad)

soros ütemezés:olyan ütemezés, amikor a különböző tranzakciók utasításai nem keverednek, először lefut az egyik összes utasítása, aztán a másiké, aztán a harmadiké, . . .

sorosítható ütemezés: olyan ütemezés, amelynek hatása azonos a résztvevő tranzakciók **valamely** soros ütemezésének hatásával (azaz a végén minden érintett adatelem pont úgy néz ki, mint a soros ütemezés után)

Sorosíthatóság

Megjegyzés: Az mindegy, hogy melyik soros ütemezéssel lesz ekvivalens a sorosítható ütemezés. Mivel a soros ütemezésekről feltettük, hogy jók, ezért ha valamelyikkel ekvivalens, az már elég.

Cél: olyan sorrend (összefésülődés) kikényszerítése, ami sorosítható ütemezés

Módszer: az ütemező (az adatbáziskezelő része) felelős azért, hogy csak ilyen sorrendek legyenek. Figyeli a tranzakciók műveleteit és késleltet/ABORT-ál tranzakciókat. (Nemsokára részletesebben is nézzük.)

Alapfeltevések

- feltesszük, hogy a tranzakciók elemi műveletei: adat olvasása (READ A), számolás az adattal (pl. $A++$), adat írása (WRITE A)
- a fenti elemi utasításokat tartalmazó műveletsort a lekérdezésfeldolgozó állítja elő, elemzi a magas szintű lekérdezést/módosítást és azt ilyen elemi utasításokból álló sorozattá alakítja
- természetesen megengedett, hogy több helyről olvassunk, mielőtt számolunk, megengedett, hogy több adatból számoljunk ki valamit, illetve, hogy úgy írjunk, hogy nem is olvastuk ki azt az adatot
- ha egy A adatelemet ki kell olvasni, akkor ha már a belső memóriában (pufferban) van, akkor onnan olvasunk, különben a tárkezelővel még be kell előbb hozni a háttértárról
- ha írjuk az A adatelemet, akkor alapértelmezés szerint a pufferbe írjuk, kivéve speciális eseteket, amikor elő lesz írva, hogy valami azonnal kerüljön ki biztonságos háttértárra

A tárkezelővel való együttműködés

Az előbbiek miatt az ütemező és a tárkezelő szorosan együttműködnek:

Az ütemező eszközei a sorosíthatóság elérésére

Az ütemezőnek több lehetősége is van arra, hogy kikényszerítse a sorosítható ütemezéseket:

- zárak (ezen belül is még: protokoll elemek, pl. 2PL)
- időbélyegek (time stamp)
- érvényesítés

Fő elv lesz: inkább legyen szigorúbb és ne hagyjon lefutni egy olyat, ami sorosítható, mint hogy fusson egy olyan, aki nem az.
Mindegyik technikára igaz lesz, hogy biztosra megy, azaz olyanokat is ki fog lőni, amik sorosíthatók lennének.

Példa

T_1	T_2	A	B
		x	y
Read(A,t)			
$t := t + 100$			
Write(A,t)		x+100	
	Read(A,s)		
	$s := 2 \cdot s$		
	Write(A,s)	$2 \cdot (x + 100)$	
Read(B,t)			
$t := t + 100$			
Write(B,t)			y+100
	Read(B,s)		
	$s := 2 \cdot s$		
	Write(B,s)		$2 \cdot (y + 100)$

A táblázat baloldali részén azt jelezzük, hogy milyen műveleteket végeznek a tranzakciók, a jobboldalon pedig az látszik, hogy eközben mi történik az A és B adategységekkel. Ezek kezdeti értékei x és y.

Read(A,t)= olvassuk be A értékét a t változóba
Write(A,t)= írjuk ki a t változó értékét A-ba

Látható, hogy ez nem egy soros ütemezés, mert össze vannak fésülődve a két tranzakció utasításai.

Viszont sorosítható, mert a hatása A-n és B-n is azonos a T_1T_2 soros ütemezés hatásával, (x, y)-ból $(2 \cdot (x + 100), 2 \cdot (y + 100))$ lesz.

Példa nem sorosíthatóra

T_1	T_2	A	B
Read(A,t)		x	y
$t := t + 100$			
Write(A,t)		x+100	
	Read(A,s)		
	$s := 2 \cdot s$		
	Write(A,s)	$2 \cdot (x + 100)$	
	Read(B,s)		
	$s := 2 \cdot s$		
	Write(B,s)		$2 \cdot y$
Read(B,t)			
$t := t + 100$			
Write(B,t)			$2 \cdot y + 100$

Ez nem egy sorosítható ütemezés, mert se a T_1T_2 soros ütemezés, se a T_2T_1 soros ütemezés hatása nem az, hogy (x, y)-ból $(2 \cdot (x + 100), 2 \cdot y + 100)$ lesz.

A T_1T_2 ütemezés $(2 \cdot (x + 100), 2 \cdot (y + 100))$ eredményt ad,
a T_2T_1 pedig $(2 \cdot x + 100, 2 \cdot y + 100)$-t.

Egyszerűsítések

Ha ismert, hogy mikor és mit akarnak írni és olvasni a tranzakciók és még az is ismert, hogy pontosan mit számolnak, akkor minden esetben el tudjuk dönteni, hogy egy ütemezés sorosítható-e.

A gyakorlatban azonban nem vizsgáljuk meg ennyire alaposan a történéseket, (mert pl. nem is tudnánk vagy mert az macerás), hanem az alábbi egyszerűsítésekkel dolgozunk:

- Nem vizsgáljuk meg, hogy mit számolnak a tranzakciók, hanem feltételezzük a legrosszabbat: valami olyat csinálnak a beolvasott adattal, ami teljesen egyedi. Azaz, feltesszük, hogy ha tud olyat csinálni, amitől inkonzisztens lesz a DB (az ütemezés hatása nem lesz azonos valamelyik soroséval), akkor azt teszi. $\Longrightarrow$
- Csak az írásokat és olvasásokat tartjuk nyilván, ezek alapján döntünk arról, hogy egy ütemezést sorosíthatónak tekintünk-e. Ha csak egyetlen olyan lehetséges számolás is van, amivel az írásokból és olvasásokból álló ütemezés nem sorosítható, akkor nem tekintjük sorosíthatónak.
- Ez néha kilő persze olyan ütemezéseket is, amik (ha megnéznénk a belső számolásokat is, akkor) sorosíthatók lennének, de ez nem baj.

Példák

A korábban látott két ütemezés átírva úgy, hogy a számolások ne látszódjanak:

T_1	T_2
r(A)	
w(A)	
	r(A)
	w(A)
r(B)	
w(B)	
	r(B)
	w(B)

T_1	T_2
r(A)	
w(A)	
	r(A)
	w(A)
	r(B)
	w(B)
r(B)	
w(B)	

r(A) jelentése beolvassuk A-t;
w(A) jelentése kiírjuk A-t

Látszik, hogy az első esetben bármilyen számolást is csinálnak a tranzakciók a beolvasott adattal a kiírás előtt, a számolástól függetlenül ugyanaz lesz a hatás mint a T_1T_2 soros ütemezésnél.

A második esetben, ahogy már láttuk is, lehetséges olyan számolás, ami esetén nem lesz azonos a hatás semelyik sorossal, így ez a csak írásokat és olvasásokat tartalmazó ütemezés nem sorosítható. (Persze lehetséges olyan számolás, amivel kiegészítve sorosítható lenne, de most kegyetlenek vagyunk: ha van egy olyan, amivel rossz, akkor rossz.)

Jelölés: A táblázat helyett így fogjuk az ütemezéseket megadni (a két előbbi esetben például):

$$r_1(A),\quad w_1(A),\quad r_2(A),\quad w_2(A),\quad r_1(B),\quad w_1(B),\quad r_2(B),\quad w_2(B)$$

illetve

$$r_1(A),\quad w_1(A),\quad r_2(A),\quad w_2(A),\quad r_2(B),\quad w_2(B),\quad r_1(B),\quad w_1(B)$$

Feltevések még

Általános elv (ahogy az előbb már ki is derült), hogy inkább legyünk szigorúak és minősítsünk rossznak egy olyat, ami sorosítható lenne, ha jobban megnéznénk, mint hogy sorosíthatónak mondjunk egy olyat, ami esetleg nem az $\Longrightarrow$ mindig egy erősebb feltételt fogunk tesztelni, aki ezt is túléli az biztos sorosítható.

Általában nem egy már adott ütemezésről kell eldönteni, hogy az sorosítható-e, hanem olyan technikákat, protokollokat használunk, amikkel elérjük, hogy csak sorosítható ütemezések jöjjenek létre.

Sorosíthatóság biztosítása zárakkal

Elve: A tranzakciók zárolják azokat az adatelemeket, amivel dolgoznak, és amíg valami zár alatt van, addig a többi tranzakció nem, vagy csak korlátozottan fér hozzá.

Egyszerű tranzakciómodell

Csak egyféle zárkérés van (LOCK), mindegyik művelethez ezt a zárat kell megkapni. Ezen kívül van még zárelengedés (UNLOCK). Az ütemezésekben nem csak írás és olvasás lesz, hanem a zárkérések és zárelengedések is benne lesznek. Csak olyan zárkéréseket tartalmazó ütemezéseket akarunk majd megengedni, amik eleget tesznek néhány követelménynek.
A legális ütemezés jellemzői:

1. Az i-edik tranzakció, T_i, csak akkor olvashatja vagy írhatja az A adategységet, ha előtte zárat kért és kapott rá ($LOCK_i(A)$) és a zárat még azóta nem engedte fel (nem volt még azóta $UNLOCK_i(A)$).
2. Ha T_i zárolja az A adategységet, akkor később valamikor el is kell engednie a zárat ($LOCK_i(A)$ után mindig van $UNLOCK_i(A)$).
3. Egyszerre két különböző tranzakciónak nem lehet zárja ugyanazon az adategységen.

Példa

Példa legális zárkérésre, ütemezésre ebben a modellben:

$$l_1(A),\ r_1(A),\ w_1(A),\ u_1(A),\ l_2(A),\ r_2(A),\ w_2(A),\ u_2(A),$$
$$l_1(B),\ r_1(B),\ w_1(B),\ u_1(B),\ l_2(B),\ r_2(B),\ w_2(B),\ u_2(B),$$

Példa arra, hogy hogyan dolgozhat az ütemező azon az egyszerű tranzakciómodellben, hogy legális ütemezés alakuljon ki

Tegyük fel, hogy a következő sorrendben jönnek zárkérések és műveleti kérések az ütemezőhöz (két tranzakció van):

$$l_1(A),\ r_1(A),\ w_1(A),\ l_1(B),\ u_1(A),\ l_2(A),\ r_2(A),\ w_2(A)$$

Eddig minden rendben van, minden kérést teljesíteni lehet. Ha azonban a további kérések

$$l_2(B),\ u_2(A),\ r_2(B),\ w_2(B),\ u_2(B),\quad r_1(B),\ w_1(B),\ u_1(B)$$

akkor ez már így nem mehet, mert T_2 nem kaphatja meg a kért zárat B-n, hiszen T_1 még tartja.

Emiatt az ütemező késlelteti T_2-t (T_2 vár T_1-re) és előbb engedi futni T_1-et, aztán jöhet T_2:

$$r_1(B),\ w_1(B),\ u_1(B),\ l_2(B),\ u_2(A),\ r_2(B),\ w_2(B),\ u_2(B)$$

lesz az az ütemezés, ami le fog futni, ez már legális lesz.

Holtpont

Láttuk, hogy az ütemező úgy kényszeríti ki a legális ütemezést, hogy várakoztatja a tranzakciókat. Ebből problémák lehetnek, ha a tranzakciók egymásra várnak:

Holtpont (deadlock, patt): néhány zárkérés után akkor van holtpont, ha van egy olyan részhalmaza a tranzakcióknak, akik közül egyik se tud tovább futni, mert vár egy szintén ebben a részhalmazban levő másikra (vár egy olyan zár elengedésére, amit egy másik, ebbe a részhalmazba tartozó, tranzakció tart).

Például:

$$l_1(A),\quad l_2(B),\quad l_3(C),\quad l_1(B),\quad l_2(C),\quad l_3(A)$$

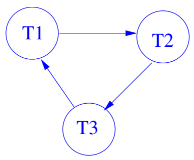
sorrendben érkező zárkérések esetén egyik tranzakció se tud tovább futni.

Az ilyen helyzeteket el kell kerülni, illetve ha már kialakultak, akkor fel kell ismerni és meg kell szüntetni.

Várakozási gráf

A felismerésben segít a zárkérések sorozatához tratozó **várakozási gráf**: csúcsai a tranzakciók és akkor van él T_i-ből T_j-be, ha T_i vár egy olyan zár elengedésére, amit T_j tart éppen.

Például az előbbi, holtponthoz vezető zárkéréssorozat várakozási gráfja a hat zárkérés után:



Vegyük észre, hogy a várakozási gráf változik az ütemezés során, ahogy újabb zárkérések érkeznek vagy zárelengedések történnek.

Holtpont felismerése

A várakozási gráf segítségével fel lehet ismerni a holtpontot az alábbi tétel miatt:

Tétel. *Az ütemezés során egy adott pillanatban pontosan akkor nincs holtpont, ha az adott pillanathoz tartozó várakozási gráf DAG (nincs benne irányított kör).*

Bizonyítás: $\Rightarrow$: Ha van irányított kör a várakozási gráfban, akkor a körbeli tranzakciók egyike se tud lefutni, mert vár a mellette levőre. Ez holtpont.
$\Leftarrow$: Ha a gráf DAG, akkor van topológikus rendezése a tranzakcióknak (lásd Algel) és ebben a sorrendben le tudnak futni a tranzakciók. (Az első nem vár senkire, mert nem megy belőle ki él, így lefuthat; ezután már a másodikba se megy él, az is lefuthat . . .)

Példa

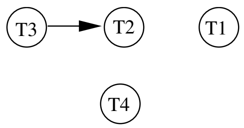
Nézzük az alábbi írásokból és olvasásokból álló ütemezést:

$$r_1(A),\quad r_2(B),\quad w_1(C),\quad r_3(D),\quad r_4(E),\quad r_3(B),\quad w_2(C),\quad w_4(A),\quad w_1(D)$$

Tegyük fel, hogy a zárkérések mindig közvetlenül megelőzik a műveletet, a zárelengedések pedig a tranzakciók végén, egyszerre történnek. Hogyan alakul a várakozási gráf ezen sorozat esetén? Lesz-e valamikor holtpont?

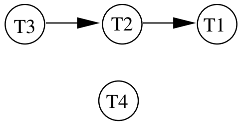
Az elején $l_1(A),\quad r_1(A),\quad l_2(B),\quad r_2(B),\quad l_1(C),\quad w_1(C),\quad l_3(D),\quad r_3(D),\quad l_4(E),\quad r_4(E)$ zárkérések és műveletek vannak, eddig még senki nem vár senkire.

Ezután $l_3(B)$ jön $r_3(B)$ miatt, de T_3-nak várnia kell T_2-re:

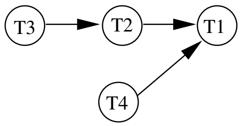


Példa

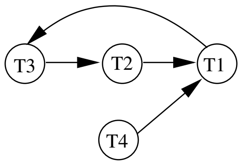
Ezután $l_2(C)$ jön $w_2(C)$ miatt, de T_2-nek is várnia kell T_1-re:



Ezután $l_4(A)$ jön $w_4(A)$ miatt, de T_4-nek is várnia kell T_1-re:



Végül $l_1(D)$ jön $w_1(D)$ miatt, de T_1-nek meg T_3-ra kell várnia:



És ez már holtpont: van irányított kör a gráfban.

Megoldások holtpont ellen

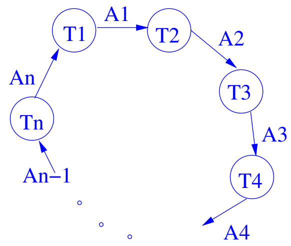
1. Rajzoljuk folyamatosan a várakozási gráfot és ha holtpont alakul ki, akkor ABORT-áljuk az egyik olyan tranzakciót, aki benne van a kialakult irányított körben.
Ez egy megengedő megoldás (optimista), hagyja az ütemező, hogy mindenki úgy kérjen zárat, ahogy csak akar, de ha baj van, akkor erőszakosan beavatkozik. Az előző példa esetében mondjuk kilövi T_2-t, ettől lefuthat T_3, majd T_1 és T_4 is.

2. Pesszimista hozzáállás: ha hagyjuk, hogy mindenki össze-vissza kérjen zárat, abból baj lehet. Előzzük inkább meg a holtpont kialakulását valahogyan. Lehetőségek:

(a) Minden egyes tranzakció előre elkéri az összes zárat, ami neki kelleni fog. Ha nem kapja meg az összeset, akkor egyet se kér el, el se indul.
Ilyenkor biztos nem lesz holtpont, mert ha valaki megkap egy zárat, akkor le is tud futni, nem akad el. Az csak a baj ezzel, hogy előre kell mindent tudni.

(b) Feltesszük, hogy van egy sorrend az adategységeken és minden egyes tranzakció csak eszerint a sorrend szerint növőleg kérhet újabb zárakat. Itt lehet, hogy lesz várakozás, de holtpont biztos nem lesz.

Bizonyítás: Ha valamely pillanatban lenne irányított kör a várakozási gráfban:



ahol T_i vár T_{i+1}-re az A_i adategység miatt, akkor $A_1 < A_2 < A_3 < \ldots A_n < A_1$ áll fenn abban az esetben, ha mindegyik tranzakció betartotta, hogy növőleg kér zárat. Ez azonban ellentmondás.

Tehát ez a protokoll is megelőzi a holtpontot, de itt is előre kell tudni, hogy milyen zárakat fog kérni egy tranzakció.

Még egy módszer, ami szintén optimista, mint az első:
Időkorlát alkalmazása: ha egy tranzakció kezdete óta túl sok idő telt el: ABORT.
Ehhez az kell, hogy ezt az időkorlátot jól tudjuk megválasztani.