

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ - ΤΜΗΥΠ

ΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ Ι

Β. Μεγαλοικονόμου
Δ. Χριστοδουλάκης

Περιορισμοί Ακεραιότητας (Integrity Constraints)

(παρουσίαση βασισμένη εν μέρη σε σημειώσεις των Silberchatz, Korth και Sudarshan και του C. Faloutsos)



Γενική Επισκόπηση

- Τυπικές γλώσσες ερωτημάτων
 - Σχεσιακή άλγεβρα και λογισμός
- Εμπορικές γλώσσες ερωτημάτων
 - SQL
 - QBE, (QUEL)
- **Περιορισμοί Ακεραιότητας**
- Συναρτησιακές Εξαρτήσεις
- Κανονικοποίηση –*καλός* σχεδιασμός ΒΔ



Περιορισμοί:

Περιορισμοί ακεραιότητας στο E-R μοντέλο:

- Κλειδί
- Λόγος πληθικότητας μιας συσχέτισης



Επισκόπηση

- Περιορισμοί πεδίου, περιορισμοί αναφορικής ακεραιότητας (Referential Integrity constraints)
- Βεβαιώσεις (assertions) και Σκανδάλες (triggers)
- Συναρτησιακές Εξαρτήσεις (Functional dependencies)



Περιορισμοί Πεδίου

- Τύποι πεδίου, π.χ. SQL
 - Χαρακτήρες ορισμένου μήκους
 - Int, float, (date)
- Τιμές null π.χ.
 - `create table φοιτητής(AM char(9) not null, ...)`

Περιορισμοί αναφορικής ακεραιότητας

'foreign keys' – πχ.

create table παίρνει(

ΑΜ **char(9) not null,**

κωδ **char(5) not null,**

βαθμός **integer,**

primary key(ΑΜ, κωδ),

foreign key ΑΜ **references** φοιτητής,

foreign key κωδ **references** μάθημα)



Περιορισμοί αναφορικής ακεραιότητας

...

foreign key AM references φοιτητής,
foreign key κωδ references μάθημα)

Επακόλουθο:

- Αναμένει ότι το AM θα υπάρχει στον πίνακα 'φοιτητής'
- Εμποδίζει λειτουργίες που το παραβιάζουν – πώς;;
 - Εισαγωγή;
 - Διαγραφή/ Ενημέρωση;



Περιορισμοί αναφορικής ακεραιότητας

...

foreign key AM references φοιτητής
on delete cascade
on update cascade,

...

- → απομάκρυνε όλες τις εγγραφές φοιτητών
- Άλλες επιλογές (set to null, to default, κα.)

Όπλα για τους περιορισμούς ακεραιότητας

■ Βεβαιώσεις (assertions)

- **create assertion** <όνομα-βεβαίωσης>
check <κατηγορία>
- Υψηλό κόστος ελέγχου και διατήρησης βεβαιώσεων

■ Σκανδάλες (triggers) (~ 'ισχυρές' βεβαιώσεις)

- Για την ενεργοποίηση, if **συνθήκη** then **δράση**
- Το σύστημα εκτελεί τη δράση αυτόματα σαν παρενέργεια μιας τροποποίησης στη ΒΔ

Βεβαιώσεις - παράδειγμα

- Το συνολικό ποσό όλων των δανείων σε κάθε υποκατάστημα πρέπει να είναι μικρότερο από το συνολικό ποσό όλων των λογαριασμών στο υποκατάστημα

```
create assertion sum-constraint check  
  (not exists (select * from υποκατάστημα  
    where (select sum(ποσό) from δάνειο  
      where δάνειο.όνομα-υποκαταστήματος =  
        υποκατάστημα.όνομα-υποκαταστήματος)  
    >= (select sum(ποσό) from λογαριασμός  
      where δάνειο.όνομα-υποκαταστήματος =  
        υποκατάστημα.όνομα-υποκαταστήματος)))
```



Σκανδάλες - παράδειγμα

```
define trigger μηδενικόςβαθμός on update  
    παίρνει  
(if new παίρνει.βαθμός < 0  
    then παίρνει.βαθμός = 0)
```

Σκανδάλες - συζήτηση

- Περισσότερο πολύπλοκες: “οι manager έχουν υψηλότερους μισθούς από τους υφισταμένους τους” – μία σκανδάλη μπορεί αυτόματα να δώσει ώθηση στους μισθούς των managers
- Σκανδάλες: παραπλανητικές (ατέρμονοι βρόγχοι...)

Σκανδάλες –πότε να μην χρησιμοποιούνται

■ Οι σκανδάλες χρησιμοποιούνταν αρχικά για:

- Διατήρηση περίληψης δεδομένων (π.χ. σύνολο μισθών σε κάθε τμήμα)
- Αντιγραφή ΒΔ με την καταγραφή των αλλαγών σε ειδικές σχέσεις (ονομαζόμενες **change** ή **delta** σχέσεις) και την χρήση μιας ξεχωριστής διαδικασίας για την εφαρμογή των αλλαγών σε ένα αντίγραφο

■ Σήμερα, υπάρχουν καλύτεροι τρόποι για τα παραπάνω:

- Υλοποιημένες όψεις για τη διατήρηση περίληψης δεδομένων
- built-in υποστήριξη για αντιγραφή
- Ευκολίες ενθυλάκωσης χρησιμοποιούνται αντί για σκανδάλες (π.χ. ορίζουν μεθόδους για την ενημέρωση πεδίων και την εκτέλεση δράσεων ως μέρος των μεθόδων ενημέρωσης αντί της χρήσης σκανδάλης)



Επισκόπηση

- Πεδίο, Περιορισμοί αναφορικής ακεραιότητας
- Βεβαιώσεις και Σκανδάλες
- Ασφάλεια
- Συναρτησιακές Εξαρτήσεις
 - Γιατί
 - Ορισμός
 - Τα αξιώματα Armstrong
 - Κλειστότητα και κάλυμμα



Ασφάλεια

- Προστασία από κακόβουλες απόπειρες υποκλοπής ή τροποποίησης των δεδομένων
 - Επίπεδο βάσης δεδομένων
 - Μηχανισμοί πιστοποίησης (authentication) και εξουσιοδότησης (authorization): επιτρέπουν σε συγκεκριμένους χρήστες να έχουν πρόσβαση μόνο στα απαιτούμενα δεδομένα
 - Εστιάζουμε στην εξουσιοδότηση
 - Επίπεδο λειτουργικού συστήματος
 - Επίπεδο δικτύου
 - Φυσικό επίπεδο
 - Ανθρώπινο επίπεδο



Εξουσιοδότηση

Μορφές εξουσιοδοτήσεων στα μέρη της ΒΔ:

- **Read authorization** – ανάγνωση αλλά όχι τροποποίηση
- **Insert authorization** – εισαγωγή νέων δεδομένων αλλά όχι τροποποιήσεις στα υπάρχοντα δεδομένα
- **Update authorization** – τροποποίηση αλλά όχι διαγραφή δεδομένων
- **Delete authorization** – διαγραφή δεδομένων

Εξουσιοδότηση (συνέχεια)

Μορφές εξουσιοδοτήσεων για την τροποποίηση του σχήματος της ΒΔ:

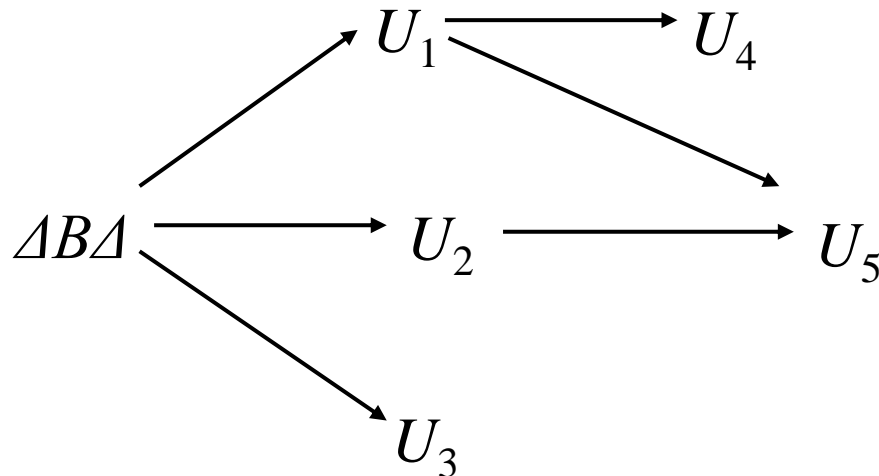
- **Index authorization** – δημιουργία, διαγραφή ευρετηρίων
- **Resources authorization** – δημιουργία νέων σχέσεων
- **Alteration authorization** – εισαγωγή ή διαγραφή γνωρισμάτων σε μία σχέση
- **Drop authorization** – διαγραφή σχέσεων

Εξουσιοδότηση και Όψεις

- Οι χρήστες μπορεί να έχουν εξουσιοδότηση σε όψεις αντί για εξουσιοδότηση σε σχέσεις
- Η ικανότητα των όψεων για απόκρυψη δεδομένων αυξάνει την ασφάλεια
- Συνδυασμός ασφάλειας στο επίπεδο σχέσεων και στο επίπεδο όψεων
- Η δημιουργία όψης δεν απαιτεί εξουσιοδότηση **πόρων** εφόσον δε δημιουργείται καμιά πραγματική σχέση

Μεταβίβαση προνομίων

- Γράφος εξουσιοδότησης: αναπαριστά τη μεταβίβαση της εξουσιοδότησης από τον ένα χρήστη στον άλλον
- κόμβοι \leftrightarrow χρήστες
- ρίζα \leftrightarrow διαχειριστής βάσης δεδομένων
- Θεωρείστε ένα γράφο για την ενημέρωση της εξουσιοδότησης στο δάνειο
- Μια ακμή $U_i \rightarrow U_j$ δηλώνει ότι ο χρήστης U_i έχει εξουσιοδοτήσει με το προνόμιο της ενημέρωσης στο δάνειο τον χρήστη U_j .



Γράφος Μεταβίβασης Προνομίων

- Προ-απαιτούμενο: όλες οι ακμές σε έναν γράφο εξουσιοδότησης πρέπει να είναι μέρος κάποιου μονοπατιού που ξεκινά από τον ΔΒΔ
- Αν ο ΔΒΔ ανακαλέσει το προνόμιο του χρήστη U_1 :
 - Το προνόμιο πρέπει να ανακληθεί από τον U_4 εφόσον ο U_1 δεν έχει πια εξουσιοδότηση
 - Το προνόμιο δεν πρέπει να ανακληθεί από τον U_5 εφόσον ο U_5 έχει κι άλλο μονοπάτι εξουσιοδότησης από τον ΔΒΔ μέσω του χρήστη U_2
- Πρέπει να αποφεύγονται κύκλοι στις μεταβιβάσεις που δεν έχουν μονοπάτι από τη ρίζα:
 - Ο ΔΒΔ μεταβιβάζει εξουσιοδότηση στο χρήστη U_7
 - Ο χρήστης U_7 μεταβιβάζει εξουσιοδότηση στο χρήστη U_8
 - Ο χρήστης U_8 μεταβιβάζει εξουσιοδότηση στο χρήστη U_7
 - Ο ΔΒΔ ανακαλεί την εξουσιοδότηση από τον χρήστη U_7
- Πρέπει να ανακαλέσει την εξουσιοδότηση από τον U_7 στον U_8 και από τον U_8 στον U_7 εφόσον δεν υπάρχει πια μονοπάτι από τον ΔΒΔ στον U_7 ή στον U_8

Απαιτήσεις Ασφάλειας στην SQL

- Δήλωση μεταβίβασης για την απονομή εξουσιοδότησης
grant <λίστα προνομίων>
on <όνομα σχέσης ή όνομα όψης> **to** <λίστα χρηστών>
- Η <λίστα χρηστών> είναι:
 - Ένας κωδικός χρήστη (user-id)
 - *public*, επιτρέπει σε όλους τους νόμιμους χρήστες το προνόμιο της μεταβίβασης
 - Ένας ρόλος (role) (... περισσότερα στη συνέχεια)
- Η μεταβίβαση ενός προνομίου σε μία όψη **δεν υπονοεί** μεταβίβαση κάποιων προνομίων στις αντίστοιχες σχέσεις
- Ο μεταβιβαστής του προνομίου πρέπει ήδη να κατέχει το προνόμιο στο προσδιοριζόμενο στοιχείο

Προνόμια στην SQL

- **select:** δυνατότητα ανάγνωσης μιας σχέσης ή δυνατότητα υποβολής ερώτησης με τη χρήση της όψης
 - Πχ. grant χρήστες U_1 , U_2 , και U_3 **select** εξουσιοδότηση στη σχέση *υποκατάστημα*:
grant select on υποκατάστημα to U_1 , U_2 , U_3
- **insert:** δυνατότητα εισαγωγής πλειάδων
- **update:** δυνατότητα ενημέρωσης με χρήση της SQL πρότασης update
- **delete:** δυνατότητα διαγραφής πλειάδων
- **references:** δυνατότητα δήλωσης foreign keys κατά τη δημιουργία σχέσεων
- **all privileges:** χρησιμοποιείται σαν ένας σύντομος τύπος για όλα τα επιτρεπόμενα προνόμια

Προνόμιο Μεταβίβασης Προνομίων

- **with grant option:** επιτρέπει σε έναν χρήστη που του έχει δοθεί ένα προνόμιο να μεταβιβάσει το προνόμιο σε άλλους χρήστες

- Π.χ.

grant select on υποκατάστημα to U_1 with grant option

Δίνει στο χρήστη U_1 το προνόμιο του **select** στον πίνακα υποκατάστημα και επιτρέπει στον U_1 να μεταβιβάσει αυτό το προνόμιο σε άλλους

Ρόλοι

- Η άδεια για κοινά προνόμια σε μια **κλάση χρηστών** μπορεί να προσδιοριστεί μια φορά με τη δημιουργία του αντίστοιχου «*ρόλου*»
- Τα προνόμια μπορεί να μεταβιβαστούν ή να ανακληθούν από ρόλους όπως και από χρήστη
- Οι ρόλοι αναθέτονται σε χρήστες ή ακόμα και σε άλλους ρόλους
- SQL:1999 υποστηρίζει ρόλους

create role *ταμείας*

create role *διαχειριστής*

grant select on *υποκατάστημα* **to** *ταμείας*

grant update (*υπόλοιπο*) **on** *λογαριασμός* **to** *ταμείας*

grant all privileges on *λογαριασμός* **to** *διαχειριστής*

grant *ταμείας* **to** *διαχειριστής*

grant *ταμείας* **to** *Αλίκη, Βασίλης*

grant *διαχειριστής* **to** *Ανδρέας*

Ανάκληση Εξουσιοδότησης στην SQL

- Η πρόταση **revoke** χρησιμοποιείται για την ανάκληση εξουσιοδότησης
revoke<λίστα προνομίων>
on <όνομα σχέσης ή όνομα όψης> **from** <λίστα χρηστών>
[restrict|cascade]

Πχ. **revoke select on υποκατάστημα from U_1, U_2, U_3 cascade**

- Η ανάκληση του προνομίου από έναν χρήστη μπορεί να οδηγήσει και άλλους χρήστες να χάσουν τα προνόμιά τους, κάτι που αναφέρεται ως κλιμάκωση της **revoke**
- Μπορούμε να αποτρέψουμε την κλιμάκωση με τον προσδιορισμό **restrict**:

revoke select on branch from U_1, U_2, U_3 restrict

Με το **restrict**, η εντολή **revoke** αποτυγχάνει αν απαιτηθούν κλιμακωτές ανακλήσεις

Ανάκληση Εξουσιοδότησης στην SQL (συνέχεια)

- <λίστα-προνομίων> μπορεί να είναι **all** για την ανάκληση όλων των προνομίων που έχει κάποιος χρήστης
- Αν η <λίστα-ανάκλησης> περιλαμβάνει το **public** όλοι οι χρήστες χάνουν το προνόμιο εκτός από εκείνους που τους απονεμήθηκε ρητά
- Αν το ίδιο προνόμιο απονεμήθηκε δύο φορές στον ίδιο χρήστη από διαφορετικούς μεταβιβαστές, ο χρήστης μπορεί να διατηρήσει το προνόμιο μετά την ανάκληση
- Όλα τα προνόμια που είναι εξαρτημένα από το προνόμιο που ανακλήθηκε, ανακαλούνται κι αυτά

Περιορισμοί Εξουσιοδότησης στην SQL

- Η SQL **δεν** υποστηρίζει εξουσιοδότηση σε επίπεδο πλειάδας
 - Π.χ. για να περιορίσουμε τους φοιτητές στο να βλέπουν μόνο (τις πλειάδες που αποθηκεύουν) τους δικούς τους βαθμούς
- Όλοι οι τελικοί χρήστες μιας εφαρμογής (π.χ. μιας δικτυακής εφαρμογής) μπορεί να **αντιστοιχίζονται σε έναν χρήστη ΒΔ**
- Στις παραπάνω περιπτώσεις, **το έργο της εξουσιοδότησης επωμίζεται το πρόγραμμα εφαρμογής**, χωρίς υποστήριξη από την SQL
 - Η εξουσιοδότηση συντελείται στον κώδικα της εφαρμογής και μπορεί να διασκορπιστεί σε ολόκληρη την εφαρμογή
 - Ο έλεγχος για την απουσία *'παραθύρων'* εξουσιοδότησης είναι αρκετά δύσκολος



Κρυπτογράφηση

- Τα δεδομένα μπορεί να *κρυπτογραφηθούν* για πρόσθετη ασφάλεια
- Ιδιότητες μιας καλής τεχνικής κρυπτογράφησης:
 - Σχετικά απλή κρυπτογράφηση και αποκρυπτογράφηση δεδομένων
 - Το σχήμα κρυπτογράφησης εξαρτάται όχι από τη μυστικότητα του αλγορίθμου αλλά από τη μυστικότητα μιας παραμέτρου του αλγορίθμου που καλείται *κλειδί κρυπτογράφησης*
 - Είναι εξαιρετικά δύσκολο για έναν εισβολέα να προσδιορίσει το κλειδί κρυπτογράφησης

Κρυπτογράφηση (συνέχεια)

- **Data Encryption Standard (DES):** αντικαθιστά χαρακτήρες και τους επαναδιατάσσει βάσει του κλειδιού κρυπτογράφησης
 - Το κλειδί δίνεται σε εξουσιοδοτημένους χρήστες μέσω ενός ασφαλούς μηχανισμού
 - Το σχήμα δεν είναι πιο ασφαλές από τον μηχανισμό μετάδοσης του κλειδιού εφόσον το κλειδί πρέπει να μοιραστεί
- **Advanced Encryption Standard (AES):** είναι ένα νέο standard που αντικαθιστά το DES και στηρίζεται στον αλγόριθμο Rijndael (επίσης εξαρτάται από τα διαμοιραζόμενα μυστικά κλειδιά)

Κρυπτογράφηση (συνέχεια)

- **public-key κρυπτογράφηση** –στηρίζεται στο ότι κάθε χρήστης έχει δύο κλειδιά:
 - **Δημόσιο κλειδί (public key)** – κλειδί που εκδίδεται δημόσια για την κρυπτογράφηση δεδομένων, αλλά δεν μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση δεδομένων
 - **Ιδιωτικό κλειδί (private key)** – κλειδί που είναι γνωστό σε μεμονωμένους χρήστες και χρησιμοποιείται για την αποκρυπτογράφηση δεδομένων. Δε χρειάζεται να μεταδοθεί στην πλευρά που κάνει την κρυπτογράφηση.
- Το σχήμα κρυπτογράφησης είναι τέτοιο που καθιστά αδύνατο ή εξαιρετικά δύσκολο να αποκρυπτογραφηθούν τα δεδομένα έχοντας μόνο το δημόσιο κλειδί
- Το σχήμα κρυπτογράφησης δημόσιου κλειδιού RSA στηρίζεται στη δυσκολία παραγοντοποίησης ενός πολυψήφιου ακεραίου (100-άδων ψηφίων) στα πρώτα συστατικά του



Πιστοποίηση

- Η πιστοποίηση με χρήση κωδικού (password) χρησιμοποιείται ευρέως όμως είναι επιρρεπής στην υποκλοπή του κωδικού από το δίκτυο
- Τα **Challenge-response** συστήματα αποτρέπουν τη μετάδοση κωδικών
 - Η ΒΔ αποστέλλει μια (τυχαία δημιουργημένη) συμβολοσειρά στο χρήστη
 - Ο χρήστης κρυπτογραφεί τη συμβολοσειρά και επιστρέφει το αποτέλεσμα
 - Η ΒΔ επιβεβαιώνει την ταυτότητα με την αποκρυπτογράφηση του αποτελέσματος
 - Μπορεί να χρησιμοποιηθεί ένα σύστημα κρυπτογράφησης του δημόσιου κλειδιού από τη ΒΔ που στέλνει ένα κρυπτογραφημένο μήνυμα κάνοντας χρήση του δημόσιου κλειδιού του χρήστη και ο χρήστης αποκρυπτογραφεί και στέλνει το μήνυμα πίσω

Πιστοποίηση

■ Οι Ψηφιακές Υπογραφές (digital signatures)

χρησιμοποιούνται για να επιβεβαιώσουν την αυθεντικότητα των δεδομένων

- Πχ. Χρήση ιδιωτικού κλειδιού (ανεστραμμένου) για την κρυπτογράφηση δεδομένων και επιβεβαίωση από οποιονδήποτε της αυθεντικότητας με τη χρήση του δημόσιου κλειδιού (ανεστραμμένου) για την αποκρυπτογράφηση των δεδομένων. Μόνο ο κάτοχος του ιδιωτικού κλειδιού θα μπορούσε να είχε δημιουργήσει τα κρυπτογραφημένα δεδομένα.
- Οι ψηφιακές υπογραφές μπορούν ακόμα να διασφαλίσουν **μη-αναπαραγωγή**: ο αποστολέας δεν μπορεί εκ των υστέρων να ισχυριστεί ότι δε δημιούργησε τα δεδομένα