

Mitme päringu kooskõlalisus autenditud andmebaasides

Meelis Roos

ATI seminar

20. mai 2004

Autenditud andmebaasid

- Iga päringute klassi peale ehitame autentimispuu → räsi
- Autentimispuu struktuur järgib tavaliselt indeksi struktuuri
- Filter ühe parameetri järgi: tavaline Merkle puu abil tehtud autentimispuu
- Filter mitme parameetri järgi: mitmemõõteline autentimispuu, mis autendib mingi risttahuka
- Saame kontrollida iga üksiku päringu vastuste vastavust selle päringu klassi räsile

Mitme päringu kooskõlalisus

- Olgu meil tabel T väljaga X
- Kaks päringut erinevate kasutajate poolt:
SELECT X FROM T WHERE X > 0 AND X < 10
SELECT X FROM T WHERE X > 5 AND X < 15
- Esimene tagastab {1, 3, 9}
- Teine tagastab {7, 12}
- Tahame garanteerida, et selliseid vastuolusid ei saaks tekkida

Mida tähendab kooskõlalisus?

- Ühe päringu vastuses esineva kirjega peab olema arvestatud teise päringu autentimisel kasutatava puu ehitamisel.
- Olgu meil näiteks kaks päringuklassi:

Q_1 : **SELECT** A_1, A_2 **FROM** T **WHERE**
 $l_1 \leq A_1 \leq r_1$ **AND** $l_2 \leq A_2 \leq r_2$

Q_2 : **SELECT** A_1, A_3 **FROM** T **WHERE**
 $l_4 \leq A_1 \leq r_4$ **AND** $l_3 \leq A_3 \leq r_3$

- Kui päringu q_1 vastuses sisaldub mingi kirje (a_1, a_2) , siis peab päringu q_2 puus T_2 leiduma kirje (a_1, a_3) , kus $(a_1, a_2, a_3) \in \pi_{A_1, A_2, A_3}(T)$.

Tõestamisest

- Et tõestada autentimispuude turvalisust, on vaja, et ei eksisteeriks andmebaasi T , kus me saame kahelt päringult vastused, mille tõestused aktsepteeritakse, kuid mis pole omavahel kooskõlalised.
- Iga päringute hulga puhul, kui nende tõestused aktsepteeritakse, leidub andmebaas T , milles kõik need vastused õiged on.
- Sisuliselt tahame tõetuseks konstrueerida mingi hulga päringute ja nende päringute vastuste järgi andmebaasi T , kus need päringud annaksid etteantud vastused.

Formaliseeritud eeldused 1

Olgu meil mingid konkreetsete päringute hulgad $Q_1 \subseteq Q_1$ ja $Q_2 \subseteq Q_2$. Tähistagu $R(q)$ päringu vastuseid, kus $q \in Q_1$ või $q \in Q_2$. Eeldused:

Leiduvad hulgad $L_1 \subseteq A_1 \times A_2$ ja $L_2 \subseteq A_1 \times A_3$ (L_i nagu *leaves*, T_i lehed) nii, et:

$$\forall a_1, a_2 : (a_1, a_2) \in L_1 \Rightarrow \\ \forall q \in Q_1, \text{ kus } l_1^q \leq a_1 \leq r_1^q \text{ ja } l_2^q \leq a_2 \leq r_2^q : (a_1, a_2) \in R(q)$$

$$\forall a_1, a_3 : (a_1, a_3) \in L_2 \Rightarrow \\ \forall q \in Q_2, \text{ kus } l_4^q \leq a_1 \leq r_4^q \text{ ja } l_3^q \leq a_3 \leq r_3^q : (a_1, a_3) \in R(q)$$

Formaliseeritud eeldused 2

$$\exists q \in Q_1 : (a_1, a_2) \in R(q) \Rightarrow (a_1, a_2) \in L_1$$

$$\exists q \in Q_2 : (a_1, a_3) \in R(q) \Rightarrow (a_1, a_3) \in L_2$$

$$\forall a_1, a_2, ((\exists q \in Q_1 : (a_1, a_2) \in R(q)) \Rightarrow \exists b : (a_1, b) \in L_2)$$

$$\forall a_1, a_3, ((\exists q \in Q_2 : (a_1, a_3) \in R(q)) \Rightarrow \exists b : (a_1, b) \in L_1)$$

Formaliseeritud eeldused 3

Päringuvastuste piires kehtivad järgmised tingimused:

$$\forall a_1, a_2, (a_1, a_2) \in R(q) \Rightarrow l_1^q \leq a_1 \leq r_1^q, l_2^q \leq a_2 \leq r_2^q$$

$$\forall a_1, a_3, (a_1, a_3) \in R(q) \Rightarrow l_4^q \leq a_1 \leq r_4^q, l_3^q \leq a_3 \leq r_3^q$$

Algoritm tabeli T koostamiseks

- Koostame hulgad L_i iga päringuklassi kohta
- Esiteks lisame L_i sisse kõik päringuvastused: $L'_i := \cup R(q)$, kus $q \in Q_i$
- Teiseks korjame kõik kirjed kooskõlalisuse tingimuste järgi
- Kontrollime ülejäänud eelduste täidetust

Näide: päringud

q_1 : **select** A_1, A_2 **from** T **where** $0 \leq A_1 \leq 2$ **and** $2 \leq A_2 \leq 4$

q_2 : **select** A_1, A_2 **from** T **where** $0 \leq A_1 \leq 3$ **and** $0 \leq A_2 \leq 1$

q_3 : **select** A_1, A_2 **from** T **where** $1 \leq A_1 \leq 4$ **and** $0 \leq A_2 \leq 3$

q_4 : **select** A_1, A_3 **from** T **where** $1 \leq A_1 \leq 3$ **and** $1 \leq A_3 \leq 2$

q_5 : **select** A_1, A_3 **from** T **where** $2 \leq A_1 \leq 4$ **and** $1 \leq A_3 \leq 3$

q_6 : **select** A_1, A_3 **from** T **where** $0 \leq A_1 \leq 1$ **and** $-\infty \leq A_3 \leq$

∞

Näide: päringuvastused

- $R(q_1) = \{(0, 4), (1, 2)\}$
- $R(q_2) = \{(0, 1), (2, 0)\}$
- $R(q_3) = \{(1, 2), (2, 0), (4, 3)\}$
- $R(q_4) = \{(1, 1), (3, 2)\}$
- $R(q_5) = \{(3, 2), (4, 2)\}$
- $R(q_6) = \{(0, 0), (1, 1)\}$

Näide: konstrueerimine

- $L'_1 = \{(0, 1), (0, 4), (1, 2), (2, 0), (4, 3)\}$
- $L'_2 = \{(0, 0), (1, 1), (3, 2), (4, 2)\}$
- $L_1 := L'_1 \cup \{(0, b_1), (1, b_2), (3, b_3), (4, b_4)\}$
- $L_2 := L'_2 \cup \{(0, c_1), (1, c_2), (2, c_3), (4, c_4)\}$

Näide: tabel T

A_1	0	0	1	2	4	0	1	1	3	4
A_2	1	4	2	0	3	b_1	b_2	b_2	b_3	b_4
A_3	c_1	c_1	c_2	c_3	c_4	0	1	3	2	2

Näide: kontroll

- Eeldusi kontrollides leiame, et q_1 kuni q_5 vastused klappivad, aga q_6 vastuseks tuleb $\{(0, 0), (1, 1), (0, c_1), (1, c_2)\}$
- Võtame $c_1 = 0$ ja $c_2 = 1$
- Kui aga venitada q_1 ja q_6 sees A_1 alumist piiri -1 peale ja tuua q_1 vastusesse juurde kirje $(-1, 3)$, siis nii ei saa: -1 puudub q_6 vastustes
- Lahenduseks on eelduste täidetust enne L_i konstrueerimist kontrollida

Päringuvastuse suurus ühe kirje kohta

- Kirje suurus — vastus ise
- Tõestus autentimispuust — puu T_i kõrgus \times lehe maht (lehed on tabeli T projektsioonist Q_i väljade järgi, näiteks $\pi_{A_1, A_2}(T)$)
- Üks "b" iga erineva päringutüübi kohta
- Privaatsusprobleem