連言問合せ間の解像度高低関係成立のための必要十分条件に関する考察

松村　卓朗† 　橋本　健二†† 　石原　靖哲† 　藤原　融†

† 大阪大学 大学院情報科学研究科　〒 565-0871 大阪府吹田市山田丘 1-5
†† 奈良先端科学技術大学院大学 情報科学研究科　〒 630-0192 奈良県生駒市高山町 8916-5
E-mail: †{t-matumr,ishihara,fujiwara}@ist.osaka-u.ac.jp, ††k-hasimt@is.naist.jp

あらまし　筆者らは，データベースへの推論攻撃に対して,「問合せ解像度の高低関係」という概念に基づくインスタンス独立な安全性定義を提案している．しかし関係データベースにおける問合せ解像度の性質についてはほとんど明らかにされていなかった．本稿では連言問合せを対象とし，まず問合せ解像度に関連するいくつかの性質を示す．次に，ある前提条件のもとで，問合せ間の解像度高低関係が成立するための判定可能な必要十分条件を与える．
キーワード　データベースセキュリティ，推論攻撃，問合せ解像度，インスタンス独立，連言問合せ

A study on a necessary and sufficient condition for existence of resolution relation between two conjunctive queries

Takuro MATSUMURA†, Kenji HASHIMOTO††, Yasunori ISHIHARA†, and Toru FUJIWARA†

† Graduate School of Information Science and Technology, Osaka University
1-5 Yamadaoka, Suita, Osaka 565-0871, Japan
†† Graduate School of Information Science, Nara Institute of Science and Technology
8916-5 Takayama, Ikoma, Nara 630-0192, Japan
E-mail: †{t-matumr,ishihara,fujiwara}@ist.osaka-u.ac.jp, ††k-hasimt@is.naist.jp

Abstract　Against inference attacks on databases, we have proposed instance-independent security definitions based on a concept of “query resolution”. However, we have not explored properties of query resolution of relational databases. In this paper, we focus on conjunctive queries and show some properties of query resolution. Then, under some assumptions, we propose a decidable necessary and sufficient condition for existence of resolution relation between two conjunctive queries.
Key words　database security, inference attack, query resolution, instance-independent, conjunctive query

1. ま え が き

データベースセキュリティを達成する上で重要な課題のひとつに，推論攻撃に対する安全性の確保がある．推論攻撃とは，ユーザが，実行を許可された問合せのみを用いて，許可されていない問合せの実行結果を推論することをいう．これまでに推論攻撃に対する安全性の定義がいくつか提案されており，それらを大別すると「インスタンス依存」と「インスタンス独立」の 2 種類に分けられる．筆者らはインスタンス独立な安全性に着目した安全性定義と検証法の確立に関する研究を行っており，これまでに文献 [1] において問合せ解像度という概念を導入し，インスタンス独立な安全性の定義について検討してきた．問合せ解像度とは，あるデータベーススキーマに従うデータベースインスタンス集合に対する，問合せ q の問合せ結果に基づく同値類分割である (図 1)．q の問合せ結果による同値類分割より

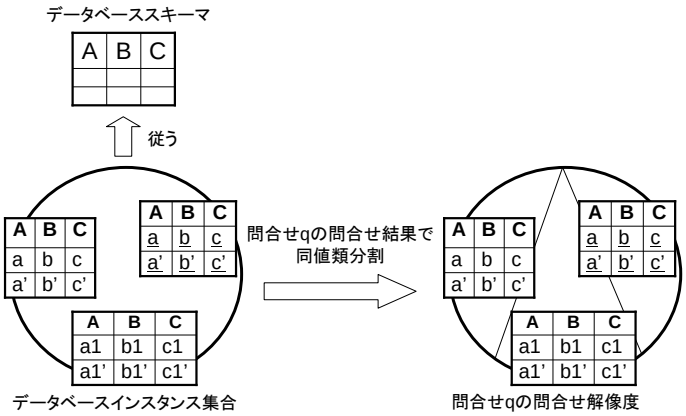

図 1　問合せ q の問合せ解像度イメージ

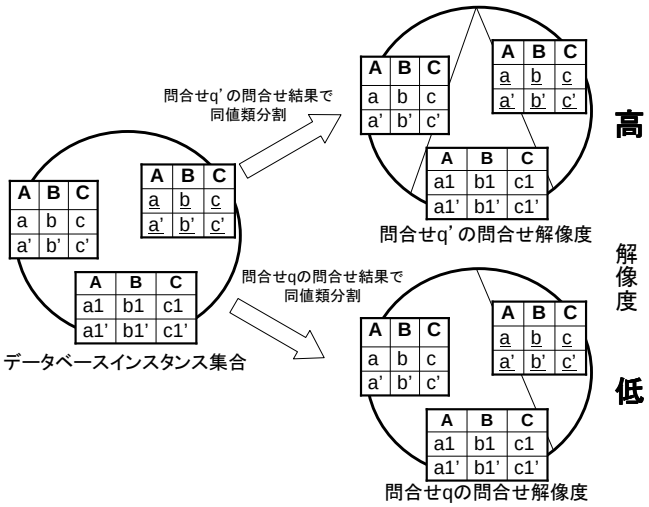

図 2　問合せ解像度の高低関係イメージ

q' の問合せ結果による同値類分割のほうが真に細かいとき，q' は q より解像度が高い (図 2) といい $q \preceq q'$ と表現する．

直観的には，問合せ結果ごとにインスタンスのグループ分けを行い，q が 2 つのインスタンス D, D' を区別できるならば，q' もインスタンス D, D' を区別できることをあらわす．文献 [1] で提案された安全性定義のうち最も単純なものは，機密情報を取り出す問合せ q_{seq} とユーザーに許可された問合せ q に $q_{seq} \preceq q$ の関係があった場合，q_{seq} は q を用いた推論攻撃に対して安全でないという定義である．これを説明するために以下の例を考える．

例 1.1. ある病院における患者の疾患状態データベースについて考える．データベースインスタンスは患者 X の疾病状態が記録されているデータとする．医師は複数人存在し，各々 *1* つの病気のみを担当するものとする．問合せ q_{sec}, q を以下に示すものとする．

q_{sec}：患者 X が患っている病気の数を返す (0 以上の値)

q：患者が掛かっている担当医師の集合を返す

このとき，q_{sec} の問合せ結果が *1* であった場合，患者 X の担当医師集合の候補 (q の問合せ結果候補) は全て要素数が *1* の集合である．同様に，q_{sec} の問合せ結果が *2* であった場合，患者 X の担当医師集合の候補 (q の問合せ結果候補) は全て要素数が *2* の集合である．このように，上記の仕様を満たす場合の疾患状態データベースについて，q の問合せ結果の同値類分割は q_{sec} の問合せ結果の同値類分割を真に細かくしたものとなっている．このとき明らかに，任意のデータベースインスタンスについて，q の問合せ結果を見れば q_{sec} の問合せ結果を一意に特定できる．

一方で，文献 [1] では，対象とする問合せは射影演算および選択演算だけであり，関係データベースなどの一般的なデータベース構造における問合せ解像度の性質については未検討であった．そこで本論文では，関係データベースにおける具体的な問合せクラスである連言問合せを対象として，問合せ解像度の高低関係が成立するための必要十分条件について考察する．

2. 関 連 研 究

本節では，まず連言問合せに関してすでに知られている基本的な性質を紹介し，次に問合せ解像度に関連する文献を紹介する．

文献 [3] は，連言問合せに関する様々な性質を示しており，その中でも，準同型写像定理が広く知られている．準同型写像定理とは，2 つの連言問合せにおける問合せ結果の包含関係と問合せ間の準同型写像の存在に関する定理で，任意の 2 つの連言問合せ q, q' において「任意のデータベースインスタンス D に対して q の問合せ結果が q' の問合せ結果に包含されるのは，問合せ q' から問合せ q に対して準同型写像が存在するときかつそのときのみである」という定理である．筆者らはすでに，問合せ間の準同型写像の存在は解像度の高低関係成立のための必要条件であるが十分条件でないことを示している．したがって，問合せ結果の包含関係と問合せ間の解像度高低関係は類似性はあるが別の概念であることが分かる．これについての具体的な説明は 4 節の冒頭で述べる．

問合せ結果にしたがって可能なインスタンス集合を同値類分割するという考え方に基づく研究として，文献 [2] がある．文献 [2] は，本報告と同じくインスタンス集合の同値類分割の考え方を用いて，攻撃者が機密情報の値をどれだけ絞り込み可能かを示す指標値を提案している．具体的には関係データベースにおいて，ある 2 つの属性集合を設定し，それぞれの属性集合の値によってインスタンス集合を同値類分割する．この 2 つの属性集合による同値類分割がどれほど重なりを持っているかを定式化し，これを片方の属性集合値からもう一方の属性集合値を推論可能かを示す指標値としている．

文献 [1] は，本報告の主題である問合せ解像度という概念を導入し，インスタンス独立な安全性定義を提案している．文献 [1] では，これまでに提案されているインスタンス独立な安全性定義の多くは，安全性要求が比較的厳しいものとなっていることに着目し，安全性要求を下げたインスタンス独立な安全性定義を提案している．

なお，以上 2 つの研究は，それぞれ異なったインスタンス独立な安全性定義を提案しているが，具体的な問合せやデータベース構造に関しては言及していない．

3. 連言問合せと問合せ解像度に関する定義と性質

本節では，まず連言問合せに関する諸定義を示した上で，その定義から導かれる連言問合せに関する 4 つの性質を示す．次に問合せ解像度の高低関係に関する定義を示す．

3.1 連言問合せに関する定義

var は変数の無限集合を表し，**dom** は定数の可算無限集合を表すとする．タプル u は $u = (e_1, e_2, \ldots, e_n)(i \in [1, n]\ e_i \in \mathbf{var} \cup \mathbf{dom})$ と定義され，テーブルはタプルの有限集合である．タプル u 中の変数の集合 $Var(u)$ は $\{x \mid x \in u \wedge x \in \mathbf{var}\}$ と定義され，また同様にテーブル T 中の変数の集合 $Var(T)$ は $\{x \mid x \in Var(u), u \in T\}$ と定義される．以上を踏まえた上で，

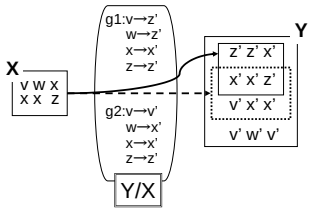

図 3　Y/X の例

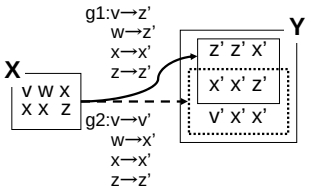

図 4　$X \mid Y$ の例

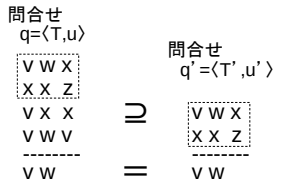

図 5　サマリが同一で，テーブル間に包含関係がある例

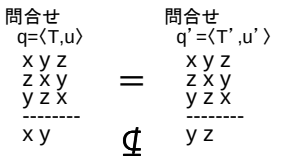

図 6　サマリに包含関係が無く，テーブルが同一である例

連言問合せに関する定義を示す.

定義 3.1. 連言問合せ q は, テーブル T とタプル u の組 $\langle T, u\rangle$ であり，u をサマリと呼ぶ．ただし，$Var(u)\subseteqq Var(T)$ である.

X, Y をタプルの集合としたとき，2 つの定義を示す.

定義 3.2. $Y/X = \{g : Var(X) \to \mathbf{var} \cup \mathbf{dom} \mid g(X)\subseteqq Y\}$. 具体的には，図 *3* のような 写像集合 $\{g1, g2\}$ を指す.

定義 3.3. $Y = \bigcup_{g\in Y/X} g(X)$ であるとき，$X \mid Y$ と書く．具体的には，図 *4* のように Y 中に X と対応が取れない部分が無い状態を指す.

以上の定義を用いて，インスタンス D に対する連言問合せ q の問合せ結果を定義する.

定義 3.4. 連言問合せ q に対し, インスタンス D を入力として与えたときの問合せ結果 $q(D)$ は $(D/T)(u)(= \{g(u) \mid g \in (D/T)\})$ と定義される.

3.2　連言問合せに関する定理と性質

まず，文献 [3] で示されている準同型写像定理を紹介する．次に，以上の連言問合せに関する定義から導かれる性質を以下に示す．なお，各性質の証明は省略する.

準同型写像定理. スキーマ R 上の任意の連言問合せ $q = \langle T, u\rangle, q' = \langle T', u'\rangle$，任意のインスタンス $D \in I(R)$ を考える．このとき，$q(D)\subseteqq q'(D)$ が成立するときかつそのときのみ, $q = \langle T, u\rangle$ から $q' = \langle T', u'\rangle$ に対して $h(T')\subseteqq T, h(u') = u$ を満たす準同型写像 $h : \mathbf{var} \to \mathbf{var} \cup \mathbf{dom}$ が存在する.

性質 3.1. 任意のインスタンス D，任意のテーブル T, T' に対して $D/T'\supseteqq(D/T) \circ (T/T')$.

性質 3.2. 任意のインスタンス D，任意のテーブル T に対して $((D/T)(T))/T = D/T$.

性質 3.3. $q = \langle T, u\rangle, Var(T) = Var(u)$ なる問合せ q と任意のインスタンス D, D' を考える．このとき $q(D) = q(D')$ となるのは $(D/T) = (D'/T)$ のとき，かつそのときのみである.

性質 3.4. 任意のテーブル T，任意のインスタンス D および $h(T)\subseteqq T$ を満たす任意の写像 $g : \mathbf{var} \to \mathbf{var} \cup \mathbf{dom}$ を考える．このとき,

$$(D/T) = (D/h(T)).$$

3.3　問合せ解像度とその高低関係に関する定義

データベース制約情報 R(スキーマ，関数従属性など) に従うデータベースインスタンスの集合を $I(R)$ と書く.

定義 3.5. 任意の連言問合せ q に対し，$q(D) = q(D')(D, D' \in I(R))$ のとき $D \equiv_{q,I(R)} D'$ と書く．$\equiv_{q,I(R)}$ により定まる $I(R)$ 上の同値類の集合を $I(R)$ における q の解像度といい，$E(q, I(R))$ と書く.

定義 3.6. 任意の連言問合せ q, q' を考える．任意の $C' \in E(q', I(R))$ に対してある $C \in E(q, I(R))$ が存在して，$C'\subseteqq C$ ならば，$I(R)$ において q' は q より解像度が高いといい，$q \preceq_{I(R)} q'$ と書く．インスタンス集合が自明なとき，または特に指定されないときは単に $q \preceq q'$ と書く．なお解像度の高低関係の式を論理式で表すと，$\forall D \in I(R), \forall D' \in I(R), q(D) \neq q(D') \Rightarrow q'(D) \neq q'(D')$ と書ける.

4.　連言問合せ間の解像度高低関係成立のための必要十分条件

本研究では，なるべく広い連言問い合わせクラスで，問合せ間の解像度の高低関係が成立するための必要十分条件を求めることを目的としている．直観的には，問合せ q に比べて問合せ q' のテーブルサイズが小さく，かつ問合せ q' のサマリの変数集合が問合せ q のサマリの変数集合を包含していれば，問合せ q' の方が問合せ q より問合せ解像度が高くなり，またその逆も成り立つと予想される．なぜならば，テーブルのサイズが小さければより多くのインスタンスに対して答えを返すことができ，またサマリの変数集合に包含関係があればインスタンスの違いをより敏感に認識できるからである．しかし，この予想は一般には正しくないことが分かっている．具体例を図 5 と図 6 で示す.

図 5 はサマリ u, u' を同一にし，テーブル T, T' に包含関係がある連言問合せの例である．しかし，この場合は問合せ間の解像度高低関係が成立しない．なぜなら図 7 のようなインスタンス D, D' を考えると，$q'(D) = q(D')$ であるが $q(D) \neq q(D')$ となっており，すなわち $q \not\preceq q'$ となるからである．また，この問合せ例には $T' = h(T')\subseteqq T, h(u') = u$ を満たす恒等写像 h が存在している．つまり，準同型写像定理より任意のインスタンス D に対して $q(D)\subseteqq q'(D)$ が成立する．以上より問合せ結果の包含関係と問合せ解像度の高低関係は類似性はあるが異なる概念であると言える.

一方，図 6 はテーブル T, T' を同一にし，サマリ u, u' 間に

	q v w x x x z v x x v w v --- v w	q' v w x x x z --- v w
D={(1,2,3), (3,3,4), (1,3,3), (1,2,1)}	q(D)= {(1,2)}	q'(D)= {(1,2),(1,3)}
D' ={(1,2,3), (3,3,4), (1,3,3)}	q(D')= ϕ	q'(D')= {(1,2),(1,3)}

図 7　図 5 中の問合せ q, q' に解像度高低関係が無いことを示すインスタンス例

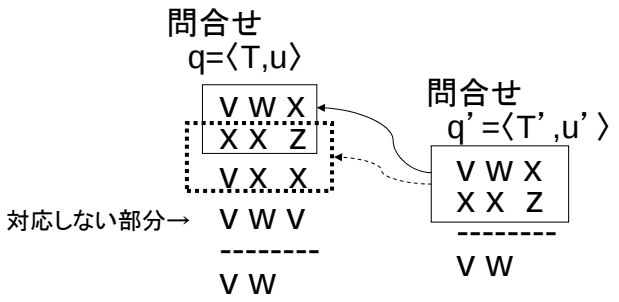

図 8　テーブル T とテーブル T' との対応関係

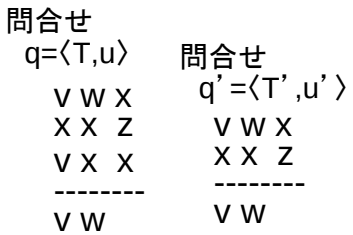

図 9　$T' \mid T$ である 2 つの連言問合せ

包含関係がない連言問合せの例である．しかしこのとき，u, u' 間に包含関係がないにもかかわらず 2 つの問合せ解像度は一致することが分かっている．

以上より，テーブル間およびサマリ間における単純な包含性だけでは問合せ間の解像度高低関係と一致しないことが分かる．よって，次節ではこれらの考察をふまえ，対象とする連言問合せのクラスをより狭めるための前提条件を置いた上で問合せ間の解像度高低関係が成立するための必要十分条件を与える．

4.1　テーブルとサマリの変数集合が一致する場合の問合せ解像度高低関係成立のための必要十分条件

図 5 の例について，問合せ間の解像度高低関係が成立しない理由は，図 8 で示すように，テーブル T 中にテーブル T' とは対応しないタプルが存在しているからである．これにより，このタプルに注目することで先のインスタンスの組 D, D' を容易に求めることができる．

次に，図 8 中の T から T' と対応付けられないタプルを除去し，$T' \mid T$ という関係が成り立つ場合 (図 9) に問合せ間の解像度高低関係が成立するかを考える．しかし，この場合も問合せ間の解像度高低関係が成立しない．なぜなら図 10 のようなインスタンス D, D' を考えると，$q'(D) = q'(D')$ であるが $q(D) \neq q(D')$ となっており，すなわち $q \not\preceq q'$ となるからである．

	q v w x x x z v x x --- v w	q' v w x x x z --- v w
D={(1,2,3), (3,3,4), (1,3,3)}	q(D)= {(1,2),(1,3)}	q'(D)= {(1,2),(1,3)}
D' ={(1,2,3), (3,3,4), (1,3,5), (5,5,6)}	q(D')= ϕ	q'(D')= {(1,2),(1,3)}

図 10　図 9 中の問合せ q, q' に解像度高低関係が無いことを示すインスタンス例

図 9 の例について，問合せ解像度高低関係が成立していない理由は，問合せ q' の問合せ結果を見ただけではテーブル T, T' の間にどのような関係があったのかが分からないからである．よって，問合せ q' の問合せ結果の集合にテーブル T, T' の間に存在している関係を確実に保持するため，サマリ u' 中の変数とテーブル T 中の変数が一致する場合を考える．この場合において問合せ間の解像度高低関係が成立するための必要十分条件を求める．ここで，テーブルが最簡であることの定義を示す．

定義 4.1. テーブル T，写像 $h : Var(T) \to \mathbf{var} \cup \mathbf{dom}$ とする．$h(T) \subseteqq T$ ならば $h(T) = T$ となるとき，T は最簡であるという．

定理 4.1. *2* つの連言問合せ $q = \langle T, u\rangle, q' = \langle T', u'\rangle$ において，$Var(u') = Var(T')$ とする．$h(T) \subseteqq T$ かつ $h(u) = u$ を満たすある準同型写像 h が存在して $T'|h(T)$ となるときかつそのときのみ $q \preceq q'$ となる．

証明． *(if part)*

性質 *3.4* より $(D/T) = (D/h(T))$ となるので，$h \circ q = \langle h(T), h(u)\rangle$ は q と同値である．$T'|h(T)$ より $(h(T)/T')(T') = h(T)$ である．ここで $q'(D) = q'(D')$ であるような任意のインスタンス D, D' を考える．$Var(u') = Var(T')$ なので，性質 *3.3* より $(D/T') = (D'/T')$ である．$D'' = (D/T')(T') = (D'/T')(T')$ とおく (D 中の，T' に当てはまらない無駄な部分が消えたものが D'')．

性質 *3.1* から

$$(D/h(T)) \circ (h(T)/T') \subseteqq (D/T'),$$
$$(D'/h(T)) \circ (h(T)/T') \subseteqq (D'/T').$$

$T' \mid h(T)$ であるので，$h(T) = (h(T)/T')(T')$ となる．よって

$$\begin{aligned}(D/h(T))(h(T)) &= (D/h(T)) \circ (h(T)/T')(T') \\ &\subseteqq (D/T')(T') = D'',\\ (D'/h(T))(h(T)) &= (D'/h(T)) \circ (h(T)/T')(T') \\ &\subseteqq (D'/T')(T') = D''.\end{aligned}$$

一方，$D'' = (D/T')(T') \subseteqq D$，$D'' = (D'/T')(T') \subseteqq D'$．$D'' \subseteqq D, D'' \subseteqq D'$ より両辺を $h(T)$ で割って，

$$(D''/h(T)) \subseteqq (D/h(T)),$$
$$(D''/h(T)) \subseteqq (D'/h(T)).$$

よって両辺に $h(T)$ をかけ，

$$(D''/h(T))(h(T)) \subseteqq (D/h(T))(h(T)) \subseteqq D'',$$
$$(D''/h(T))(h(T)) \subseteqq (D'/h(T))(h(T)) \subseteqq D''.$$

それぞれ $h(T)$ で割った式を考えると，性質 *3.2* より

$$\begin{aligned}(D''/h(T)) &= ((D''/h(T))(h(T)))/h(T)\\ &\subseteqq (D/h(T))(h(T))/h(T)\\ &\subseteqq (D''/h(T)),\\ (D''/h(T)) &= ((D''/h(T))(h(T)))/h(T)\\ &\subseteqq (D'/h(T))(h(T))/h(T)\\ &\subseteqq (D''/h(T)).\end{aligned}$$

よって $(D/h(T))(h(T))/h(T) = (D'/h(T))(h(T))/h(T)$ となるので，

$$(D/h(T)) = (D'/h(T)).$$

したがって性質 *3.3* より $h \circ q(D) = h \circ q(D')$．$h \circ q$ と q は同値であるので，$q(D) = q(D')$．

以上より $q \preceq q'$ となる．

(only if part)

背理法で示す．

$q \preceq q'$ が成立するとし，$h(T) \subseteqq T$ かつ $h(u) = u$ を満たすどんな準同型写像 h に対しても $T' \not| h(T)$ だと仮定する．$h \circ q$ が q の最簡形となる準同型写像 h を考える．

(i) $g(h(T)) \subseteqq (h(T)/T')(T')$ となる準同型写像 g が存在しない場合．

D, D' をそれぞれ $h(T), (h(T)/T')(T')$ と同型なインスタンスとする．このとき明らかに $(D/T') = (D'/T')$ なので $q'(D) = q'(D')$ となる．D は $h(T)$ と同型であるので $D/h(T) \neq \emptyset$ となるが，D' は D より真に小さく，また $g(h(T)) \subseteqq (h(T)/T')(T')$ となる準同型写像 g が存在しないので $D'/h(T) = \emptyset$ となる．$h \circ q$ と q は同値であったので，$D/T \neq \emptyset, D'/T = \emptyset$ となる．

(ii) $g(h(T)) \subseteqq (h(T)/T')(T')$ となる準同型写像 g が存在する場合．

$h(q)$ が最簡であることより，どんな g も $g(h(u)) \neq h(u)$ となるはず．よって，$h(u) \in (h(T)/T)(u)$ であるが $h(u) \notin (g(h(T))/T)(u)$．$D, D'$ をそれぞれ $h(T), (h(T)/T')(T')$ と同型なインスタンスとする．このとき明らかに $(D/T') = (D'/T')$ なので $q'(D) = q'(D')$ となる．しかし $h(u) \in (h(T)/T)(u)$ であるが $h(u) \notin (g(h(T))/T)(u) \subseteqq ((h(T)/T')(T')/T)(u)$ となる．

以上の議論より $(i), (ii)$ いずれの場合においても $q'(D) = q'(D')$ であるが $q(D) \neq q(D')$ となる．よって $q \not\preceq q'$ となるが $q \preceq q'$ という前提条件と矛盾する．よって $q \preceq q'$ ならば $h(T) \subseteqq T$ かつ $h(u) = u$ を満たす準同型写像 h が存在して $T'|h(T)$ となる．

以上より $h(T) \subseteqq T$ かつ $h(u) = u$ を満たす準同型写像 h が存在して $T'|h(T)$ となるとき かつそのときのみ $q \preceq q'$ となることが示された． □

4.2 テーブルが一致する場合の問合せ解像度高低関係成立のための必要十分条件

一方，図 6 の例について，問合せ間の解像度高低関係が成立してしまう理由は，T に恒等写像以外の自己準同型写像が存在するので $(T/T)(u) = (T/T)(u')$ が成立するからである．$(T/T)(u)$ や $(T/T)(u')$ は問合せ q, q' の問合せ結果の一般型だといえる．これが同一であるから，任意のインスタンスに対して，問合せ q, q' は同一の問合せ結果を返す．よって問合せ間の解像度高低関係が一致するといえる．以上より，テーブル T に恒等写像以外の自己準同型写像が無い場合において問合せ間の解像度高低関係が成立するための必要十分条件を求める．

まず，必要十分条件を求めるために新たな記法や概念を示した上で，いくつかの補題を示す．

定義 4.2. 写像 $g : \mathbf{var} \to \mathbf{var} \cup \mathbf{dom}$ とサマリ u に対し，次のような写像を $g|_u : \mathbf{var} \to \mathbf{var} \cup \mathbf{dom}$ と表す．

$$g|_u(x) = \begin{cases} g(x) & \texttt{if } x \in Var(u) \\ x' & \texttt{otherwise} \end{cases}$$

ただし x' は T に現れない新しい変数であり，任意の $x, y \in Var(u)$ について $x \neq y$ ならば $x' \neq y'$ を満たす．

定義 4.3. 写像集合 $G = \{g : \mathbf{var} \to \mathbf{var} \cup \mathbf{dom}\}$ に対し，異なる $g|_u$, $g'|_u$ と変数 $x \notin Var(u)$ について，$g|_u(x) \neq g'|_u(x)$ を満たす写像集合 $\{g|_u \mid g \in G\}$ を $G|_u$ と表す．

定義 4.4. *2* つの連言問合せ $q = \langle T, u\rangle, q' = \langle T, u'\rangle$，写像 $f : \mathbf{var} \to \mathbf{var} \cup \mathbf{dom}$ に対し，$S_f = (f(T)/T)|_u(T)$，$S'_f = (f(T)/T)|_{u'}(T)$ と定義する．

定義 4.5. タプル集合 $c(S)$ が，$c(S) \subseteqq S$，かつある準同型写像 h に対して $c(S) = h(S)$，かつ $c(S)$ のどの真部分集合 S' とどんな準同型写像 h' に対しても $h'(S) \neq S'$ を満たすとき，$c(S)$ を S の *core* と呼ぶ．

以上の定義をふまえ，2 つの補題を示す．なお証明は紙面の都合により省略する．

補題 4.1. 任意の写像 $f : \mathbf{var} \to \mathbf{dom}$ を考える．$(f(T)/T)(u) \subseteqq (D/T)(u)$ となるとき，かつそのときのみ $(D/c(S_f)) \neq \emptyset$．

補題 4.2. *2* つの連言問合せ $q = \langle T, u\rangle, q' = \langle T, u'\rangle$ において，T は恒等写像以外の自己準同型写像をもたないとする．ある写像 $f : \mathbf{var} \to \mathbf{dom}$ について $(c(S'_f)/c(S_f)) = \emptyset$ ならば，ある g, h が存在して $(g(T)/T)(u') = (h(T)/T)(u')$ かつ $(g(T)/T)(u) \neq (h(T)/T)(u)$．

以上の定義および補題を用いて，2 つ目の問合せ間の問合せ解像度高低関係成立のための必要十分条件を示す．

定理 4.2. *2* つの連言問合せ $q = \langle T, u\rangle, q' = \langle T, u'\rangle$ において，T は恒等写像以外の自己準同型写像をもたないとする．このとき，$q \preceq q'$ となるのは任意の写像 $f : \mathbf{var} \to \mathbf{dom}$ に対して $(c(S'_f)/c(S_f)) \neq \emptyset$ となるときかつそのときのみ．

証明 . *(if part)*

任意の写像 $f : \mathbf{var} \to \mathbf{dom}$ に対して $(c(S'_f)/c(S_f)) \neq \emptyset$ であるとする．$(D/T)(u) \neq (D'/T)(u)$ を満たす任意の D, D' を考える．一般性を失うことなく，

$$(g(T)/T)(u) \subseteq (D/T)(u),$$
$$(g(T)/T)(u) \not\subseteq (D'/T)(u)$$

をともに満たすような写像 $g \in (D/T)$ が存在するといえる．ここで，$(D/T)(u') = (D'/T)(u')$ であると仮定する．$g \in (D/T)$ より $g(T) \subseteq D$ であるので $(g(T)/T)(u') \subseteq (D/T)(u')$ となる．したがって，g は，

$$g(T) \not\subseteq D',$$
$$(g(T)/T)(u') \subseteq (D'/T)(u')$$

の両方を満たさなくてはならない．$(g(T)/T)(u') \subseteq (D'/T)(u')$ と補題 *4.1* より，

$$(D'/c(S'_g)) \neq \emptyset.$$

仮定より，$(c(S'_g)/c(S_g)) \neq \emptyset$ であるので，$(D'/c(S_g)) \neq \emptyset$ となる．よって補題 *4.1* より $(g(T)/T)(u) \subseteq (D'/T)(u)$ となる．しかしこれは g の性質 $(g(T)/T)(u) \not\subseteq (D'/T)(u)$ に矛盾する．したがって $(D/T)(u') \neq (D'/T)(u')$ であり，$q \preceq q'$ が導ける．

(only if part)

対偶を示す．すなわち「ある写像 $f : \mathbf{var} \to \mathbf{dom}$ について $(c(S'_f)/c(S_f)) = \emptyset$ ならば $q \not\preceq q'$」を示す．

ある写像 $f : \mathbf{var} \to \mathbf{dom}$ に対して $(c(S'_f)/c(S_f)) = \emptyset$ であるとき，補題 *4.2* より，ある g, h が存在して，$(g(T)/T)(u') = (h(T)/T)(u')$ かつ $(g(T)/T)(u) \neq (h(T)/T)(u)$ となる．このとき，$D = g(T), D' = h(T)$ とおくと明らかに $(D/T)(u) \neq (D'/T)(u)$ かつ $(D/T)(u') = (D'/T)(u')$．よって，ある写像 $f : \mathbf{var} \to \mathbf{dom}$ について $(c(S'_f)/c(S_f)) = \emptyset$ ならば $q \not\preceq q'$ となる．

以上より，$q \preceq q'$ となるのは任意の写像 $f : \mathbf{var} \to \mathbf{dom}$ に対して $(c(S'_f)/c(S_f)) \neq \emptyset$ となるときかつそのときのみであることが示された． □

4.3 問合せに対称性が無い場合の問合せ解像度高低関係成立のための必要十分条件

以上 2 つの問合せ解像度高低関係成立のための必要十分条件は，対象とする連言問合せに対して極めてきびしい制限をおいている．よって，対象とする連言問合せクラスを広げる目的で，問合せに対称性が無い場合の問合せ解像度高低関係成立のための必要十分条件を求める．

まず，必要十分条件を求めるために新たな記法を定義した上で，いくつかの補題を示す．なお証明は紙面の都合により省略する．

定義 4.6. *2* つの連言問合せ $q = \langle T, u\rangle, q' = \langle T', u'\rangle$，写像 $f : \mathbf{var} \to \mathbf{var} \cup \mathbf{dom}$ に対し，$S''_f = (f(T)/T')|_{u'}(T')$ と定義する．

補題 4.3. *2* つの連言問合せ $q = \langle T, u\rangle, q' = \langle T', u'\rangle$ と任意のインスタンス D, D' を考える．$q(D) \neq \emptyset$ とする．$h(T) \subseteq T, h(u) = u$ なる写像 h が存在し，$T' \mid h(T)$ とする．任意の異なる写像 $g_1, g_2 \in (T/T')$ について，$Var(g_1(T')) \cap Var(g_2(T')) \subseteq Var(g_1(u')) \cup Var(g_2(u'))$ とする．このとき，

$$q'(D) = q'(D') \text{ ならば } q(D') \neq \emptyset$$

補題 4.4. 任意の写像 $f : \mathbf{var} \to \mathbf{dom}$，*2* つの連言問合せ $q = \langle T, u\rangle, q' = \langle T', u'\rangle$，任意のインスタンス D を考える．任意の異なる写像 $h_1, h_2 \in (T/T')$ について $h_1(T') \cap h_2(T') = \emptyset$ であり $T' \mid T$ とする．このとき，

$$(f(T)/T')(u') \subseteq (D/T')(u') \text{ ならば } (D/c(S''_f)) \neq \emptyset.$$

補題 4.5. 最簡な *2* つの連言問合せ $q = \langle T, u\rangle, q' = \langle T', u'\rangle$，以下で定義される写像 $g : \mathbf{var} \to \mathbf{var}$ を考える．

$$g(x) = \begin{cases} x & \texttt{if } x \in Var(T') - Var(u') \\ x' & \texttt{otherwise} \end{cases}$$

(ただし x' は T' に現れない新しい変数)

以下の条件

(i) 任意の異なる写像 $h_1, h_2 \in (g(T)/T')$ について $h_1(T') \cap h_2(T') = \emptyset$

(ii) $T' \mid T$

(iii) 任意の写像 $h \in (T/T')$ について，$T, T', h(T'), g(T')$ は恒等写像以外の自己準同型写像をもたない

(iv) 任意の異なる写像 $g_1, g_2 \in (T/T')$ について，$Var(g_1(T')) \cap Var(g_2(T')) \subseteq Var(g_1(u')) \cup Var(g_2(u'))$

を満たすとする．このとき，ある写像 $f : \mathbf{var} \to \mathbf{dom}$ について $(c(S''_f)/c(S_f)) = \emptyset$ ならば，あるインスタンス D, D' が存在して $(D/T')(u') = (D'/T')(u')$ かつ $(D/T)(u) \neq (D'/T)(u)$.

以上の定義および補題を用いて，3 つ目の問合せ間の問合せ解像度高低関係成立のための必要十分条件を示す．

定理 4.3. 最簡な *2* つの連言問合せ $q = \langle T, u\rangle, q' = \langle T', u'\rangle$，以下で定義される写像 $g : \mathbf{var} \to \mathbf{var}$ を考える．

$$g(x) = \begin{cases} x & \texttt{if } x \in Var(T') - Var(u') \\ x' & \texttt{otherwise} \end{cases}$$

(ただし x' は T' に現れない新しい変数)

以下の条件

(i) 任意の異なる写像 $h_1, h_2 \in (g(T)/T')$ について $h_1(T') \cap h_2(T') = \emptyset$

(ii) 任意の写像 $h \in (T/T')$ について，$T, T', h(T'), g(T')$ は恒等写像以外の自己準同型写像をもたない

(iii) 任意の異なる写像 $g_1, g_2 \in (T/T')$ について，$Var(g_1(T')) \cap Var(g_2(T')) \subseteqq Var(g_1(u')) \cup Var(g_2(u'))$ を満たすとする．このとき，$q \preceq q'$ となるのは $T' \mid T$ かつ任意の写像 $f : \mathbf{var} \to \mathbf{dom}$ について $(c(S''_f)/c(S_f)) \neq \emptyset$ であるときかつそのときのみ．

証明． *(if part)*

$(D/T)(u) \neq \emptyset$ となる任意のインスタンス D, D' を考える．仮にこの D, D' について $(D/T)(u) \neq (D'/T)(u), (D/T')(u') = (D'/T')(u')$ であるとする．このとき，補題 *4.3* より $(D'/T)(u) \neq \emptyset$．$(D/T)(u) \neq (D'/T)(u)$ であるので，一般性を失うことなく，

$$(g(T)/T)(u) \subseteqq (D/T)(u),$$
$$(g(T)/T)(u) \not\subseteq (D'/T)(u)$$

をともに満たすような写像 $g \in (D/T)$ が存在するといえる．$g(T) \subseteqq D$ と $(D/T')(u') = (D'/T')(u')$ より，

$$(g(T)/T')(u') \subseteqq (D/T')(u') = (D'/T')(u').$$

つまり写像 g は

$$g(T) \not\subseteq D',$$
$$(g(T)/T')(u') \subseteqq (D'/T')(u').$$

の両方を満たさなくてはならない．$(g(T)/T')(u') \subseteqq (D'/T')(u')$ であるので，補題 *4.4* より $(D'/c(S''_g)) \neq \emptyset$．前提より，任意の写像 $f : \mathbf{var} \to \mathbf{dom}$ について $(c(S''_f)/c(S_f)) \neq \emptyset$ であるので，$(c(S''_g)/c(S_g)) \neq \emptyset$ である．よって $(D'/c(S_g)) \neq \emptyset$．よって，補題 *4.1* より $(g(T)/T)(u) \subseteqq (D'/T)(u)$．しかしこれは写像 g の定義に矛盾する．

よって $(D/T')(u') = (D'/T')(u')$ ならば $(D/T)(u) = (D'/T)(u)$．すなわち $q \preceq q'$ といえる．

(only if part)

対偶を示す．すなわち「$T' \not| T$ またはある写像 f について $(c(S''_f)/c(S_f)) = \emptyset$ ならば $q \not\preceq q'$.」を示す．

(i) $T' \not| T$ のとき．

- $g(T) \subseteqq (T/T')(T')$ となる準同型写像 g が存在しない場合．

D, D' をそれぞれ $T, (T/T')(T')$ と同型なインスタンスとする．このとき明らかに $(D/T') = (D'/T')$ なので $q'(D) = q'(D')$ となる．しかし今，q は最簡形であるので $D/T \neq \emptyset, D'/T = \emptyset$ となる．

- $g(T) \subseteqq (T/T')(T')$ となる準同型写像 g が存在する場合．

q が最簡であることより，どんな g も $g(u) \neq u$ となるはず．よって，$u \in (T/T)(u)$ であるが $u \notin (g(T)/T)(u)$．D, D' をそれぞれ $T, (T/T')(T')$ と同型なインスタンスとする．このとき明らかに $(D/T') = (D'/T')$ なので $q'(D) = q'(D')$ となる．しかし $u \in (T/T)(u)$ であるが $u \notin (g(T)/T)(u) \subseteqq ((T/T')(T')/T)(u)$ となる．D, D' は $T, (T/T')(T')$ と同型なインスタンスであったので

$$u \in (D/T)(u),\ u \notin (D'/T)(u).$$

以上の議論より，どの場合においても $q'(D) = q'(D')$ であるが $q(D) \neq q(D')$ となる．よって $q \not\preceq q'$ といえる．

(ii) $T' \mid T$ かつ，ある写像 f について $(c(S''_f)/c(S_f)) = \emptyset$ のとき．

補題 *4.5* より，あるインスタンス D, D' が存在して $(D/T')(u') = (D'/T')(u')$ かつ $(D/T)(u) \neq (D'/T)(u)$ となる．つまり $q'(D) = q'(D')$ かつ $q(D) \neq q(D')$ なので $q \not\preceq q'$ といえる．

以上の議論より $(i), (ii)$ いずれの場合においても $q \not\preceq q'$ となるので，対偶「$T' \not| T$ またはある写像 f について $(c(S''_f)/c(S_f)) = \emptyset$ ならば $q \not\preceq q'$.」は示された．

以上より，$q \preceq q'$ となるのは $T'|T$ かつ任意の写像 f について $(c(S''_f)/c(S_f)) \neq \emptyset$ であるときかつそのときのみであることが示された． □

5. まとめと今後の課題

本論文では，筆者の所属する研究チームがすでに提案している「問合せ解像度」という概念を基にした，解像度の高低関係を用いた安全性定義に対して，具体的な問合せとその問合せ解像度の関係を調査した．具体的な問合せとして連言問合せに焦点を置き，連言問合せに，ある制約がある場合での解像度の高低関係が成立するための必要十分条件を与えた．

今後の課題としては，本論文で示した定理 4.1，定理 4.2，定理 4.3 で設定している制約を緩め，問合せ間の問合せ解像度高低関係が成立するための必要十分条件を求めることがあげられる．本論文で与えた 3 つの定理における前提条件は，非常に厳しいものであると考えられる．よってより広い連言問合せクラスを対象にするために，問合せに対する制約を緩め，そのうえで解像度の高低関係が成立する必要十分条件を与えたい．

文　献

[1] 廣田 祐一, 橋本 健二, 石原 靖哲, 藤原 融, “データベースへの推論攻撃に対する問合せ解像度の高低関係を用いたインスタンス独立な安全性定義の提案,” 第 1 回データ工学と情報マネジメントに関するフォーラム (DEIM2009), 2009.

[2] K. Zhang, “IRI: A quantitative approach to inference analysis in relational databases,” Proceedings of the IFIP TC11 WG11.3 Eleventh International Conference on Database Securty XI, pp. 279–290, 1997.

[3] A.K. Chandra and P.M. Merlin, “Optimal Implementation of conjunctive queries in relational databases,” Proceedings of the Ninth Annual ACM Symposium on Theory of Computing, pp. 77-90, 1977.