Journal of Universal Computer Science, vol. 4, no. 5 (1998), 547-559
submitted: 19/7/97, accepted: 19/3/93, appeared: 28/5/98 © Springer Pub. Co.

On the Number of Keys of a Relational Database Schema

Ralf Wastl
(University of Würzburg, Germany
wastl@informatik.uni-wuerzburg.de)

Abstract: We introduce an inference system for deriving all keys of a relation schema. Then we show that the number of keys of a relation schema $R = \langle U, F \rangle$ is bounded by $\lfloor e^{|F|/e} \rfloor$.
Key Words: Relation schema, keys, inference system
Category: H.2.1, H.2.8

1 Introduction

We introduce an inference system $\mathbb{K}$ for deriving keys of a relation schema $R = \langle U, F \rangle$. The entities which are derived with $\mathbb{K}$ are functional dependencies. The system $\mathbb{K}$ is sound in the sense that all functional dependencies which are derived with $\mathbb{K}$ are in F^+; $\mathbb{K}$ is complete in the sense that for every key K of R a functional dependency $K \to A$ can be derived, where $A \in U$ or $A = \varnothing$. We use the completeness of $\mathbb{K}$ to give the bound $\lfloor e^{|F|/e} \rfloor$ for the cardinality of the set of keys of R. For another bound of the set of keys of a relation schema cf. [Thalheim 1992]

We briefly collect the basic items concerning relation schemas which will be needed in this paper. For more details cf. [Maier 1983], [Ullman 1988].

An attribute A is an identifier for an element of some domain D. We use capital letters $A, B, C, D, \ldots$ for attributes. Let U be a set of attributes. An attribute set X over U is a subset of U. We use capital letters $X, Y, Z, V, \ldots$ for attribute sets. A functional dependency over U is an expression of the form $X \to Y$, where X, Y are attribute sets. Intuitively, a functional dependency $X \to Y$ means that the attribute set X determines the attribute set Y. If X, Y are attribute sets, then we write XY for $X \cup Y$. We use capital letters F, G for sets of functional dependencies over an attribute set U. We denote by $attr(F)$ the set of all attributes occurring in F. All attribute sets and all sets of functional dependencies are finite. The cardinality of a set X is denoted by $|X|$.

A relation schema $R = \langle U, F \rangle$ is an ordered pair consisting of an attribute set U and a set F of functional dependencies over U. Let $R = \langle U, F \rangle$ be a relation schema. There are distinguished subsets $K \subseteq U$, called superkeys. To define superkeys we use the algorithm *transitive closure* below. The algorithm *transitive closure* computes for an attribute set X the set $X^+ \supseteq X$ of all attributes which are functional determined by X.

Algorithm *transitive closure.*
Input: A relation schema $R = \langle U, F \rangle$ and an attribute set $X \subseteq U$.
Output: X^+.

[INIT]	$X^+ := X;$
[LOOP]	while $(\exists (Y \to Z) \in F : Y \subseteq X^+ \ \& \ Z \not\subseteq X^+)$
	$X^+ := X^+ \cup Z;$
[RESULT]	return $X^+;$

Figure 1: Algorithm *transitive closure*

Now an attribute set $K \subseteq U$ is a *superkey* of R, if $K^+ = U$. A superkey K of R is a *key* of R, if K is minimal with respect to set inclusion. Keys are also known as candidate keys. We denote the set of all keys of a relation schema R with $\mathscr{K}_R$. We use capital letters K, L for keys.

The following simple observation will be used later. The result of a computation of X^+ using the algorithm *transitive closure* does *not* depend on the sequence in which the functional dependencies are choosen in the while loop. Further, when computing the transitive closure of an attribute set X we always assume that this is done with the algorithm *transitive closure*. For a computation of X^+ we denote the LOOP–steps with $X^{(0)}, X^{(1)}, X^{(2)}, \ldots$ and so on. The inclusion $X \subseteq X^+$ is immediate. If the transitive closure of an attribute set X is computed with respect to two different sets of functional dependencies F, G, then we write $X^{+,F}$, respectively $X^{+,G}$.

We report some facts about functional dependencies. A functional dependency $X \to Y$ is trivial, if $Y \subseteq X$. Let $R = \langle U, F \rangle$ be a relation schema. The set F^+ of functional dependencies over U is defined as the set of all functional dependencies which are logically implied by F (for details [Ullman 1988]). For our concern it is relevant that the set F^+ is characterized as the set of all functional dependencies which can be derived from F using the Armstrong Axioms [Armstrong 1974]. We take the Armstrong Axioms from [Ullman 1988].

$$
\begin{array}{ll}
(\mathcal{A}1) & \varnothing \vdash_{\mathcal{A}} X \to Y \ \text{ if } Y \subseteq X \\
(\mathcal{A}2) & \{X \to Y\} \vdash_{\mathcal{A}} XZ \to YZ \ \text{ for all } Z \subseteq U \\
(\mathcal{A}3) & \{X \to Y, Y \to Z\} \vdash_{\mathcal{A}} X \to Z
\end{array}
$$

We write $F \vdash_{\mathcal{A}} X \to Y$, if there exists a formal derivation of the functional dependency $X \to Y$ from F using the Armstrong Axioms ($\mathcal{A}$1)–($\mathcal{A}$3). For details about formal derivability cf. [Mendelson 1987], for example.

When the right hand side of a functional dependency is a singleton set, then we use the notation $X \to A$, $Y \to B$, $Z \to C$ or similar. We call such functional dependencies *unit* functional dependencies.
Let $Y \to B$ be a unit functional dependency. To indicate that the attribute A occurs in the left hand side of $Y \to B$, we write $YA \to B$. Additionally, when we use the notation $YA \to B$, then we assume $A \notin Y$, that is, the union YA is disjoint. In this paper we work with unit functional dependencies. It is no restriction to consider only unit functional dependencies, see [Maier 1983] p. 77 Lemma 5.3. Further, for a relation schema $R = \langle U, F \rangle$ we always assume that $U = attr(F)$. This is no restriction when considering keys, because the attributes in $U - attr(F)$ have to be in every key of R. Summing up: For all relation schema $R = \langle U, F \rangle$ in this paper we assume that

- F is a set of non–trivial unit functional dependencies and
- $U = attr(F)$.

2 Transitive Relation Schemas

In this section we introduce the concept of a transitive relation schema, which is the key tool for proving the completeness of the inference system $\mathbb{K}$ in the next section. The relevant properties of transitive relation schemas are stated in Lemma 2 and 5.

Consider the inference rule below for infering unit functional dependencies from unit functional dependencies.

$$\frac{X \to A \qquad YA \to B}{XY \to B} \quad [B \notin X]$$

Note, that $XY \to B$ is not trivial, if $B \notin X$ and the premise functional dependencies $X \to A$, $YA \to B$ are not trivial.

We want to define the transitive closure of a set F of functional dependencies with respect to the above inference rule. Therefore, we define an operator $\mathcal{T} : F \mapsto \mathcal{T}(F)$ as

$$\mathcal{T}(F) := F \cup \{XY \to B \;\big|\; \exists (X \to A)\, \exists (YA \to B) \in F : \frac{X \to A \quad YA \to B}{XY \to B}\, [B \notin X]\}$$

The iterations of $\mathcal{T}$ are defined as

$$\begin{aligned} \mathcal{T}^{(1)}(F) &:= F \\ \mathcal{T}^{(n+1)}(F) &:= \mathcal{T}(\mathcal{T}^{(n)}(F)). \end{aligned}$$

Finally, the transitive closure $tc(F)$ of F is given as

$$tc(F) := \bigcup_{n\geq 1} \mathcal{T}^{(n)}(F).$$

Let $R = \langle U, F\rangle$ be a relation schema. We let $R^+ := \langle U, tc(F)\rangle$. R^+ is uniquely determined through R. We call R^+ the *transitive form* of R. A relation schema R is *transitive*, if $R = R^+$.

Example 1
Consider the relation schema $R = \langle\{A, B, C, D, E\}, F\rangle$, where

$$\begin{aligned} F = \{\, AB &\rightarrow C, \\ DC &\rightarrow E, \\ E &\rightarrow A\,\}. \end{aligned}$$

The transitive form of R is $R^+ = \langle\{A, B, C, D, E\}, tc(F)\rangle$, where

$$\begin{aligned} tc(F) = \{\ & AB \rightarrow C,\ DC \rightarrow E,\ E \rightarrow A, \\ & ABD \rightarrow E,\ DC \rightarrow A,\ EB \rightarrow C, \\ & DCB \rightarrow E,\ EBD \rightarrow A,\ ABD \rightarrow C\,\}.\lrcorner \end{aligned}$$

We show that the set of keys of a relation schema R coincides with the set of keys of its transitive form R^+. (Note that we work with non-trivial unit functional dependencies).

Lemma 2
Let $R = \langle U, F\rangle$ be a relation schema. Then,

$$\mathscr{K}_R = \mathscr{K}_{R^+}.$$

Proof. We show that for every attribute set $V \subseteq U$ there is

$$V^{+,F} = V^{+,tc(F)}.$$

This implies the lemma. We proceed by double induction on the well–founded set $\langle\mathbb{N}\times\mathbb{N}_0, \leq_{lex}\rangle$ and prove the following statement

$$\forall m \geq 1\, \forall n \geq 0 : V^{(n),\mathcal{T}^{(m)}(F)} \subseteq V^{(nm),F}.$$

For the inductive basis (main induction) let $m = 1$ and $n = 0$. Then $V^{(0),\mathcal{T}^{(1)}(F)} = V = V^{(0),F}$. For the inductive step (main induction) let $m + 1 > 1$. For the inductive basis (side induction) let $n = 0$. The relation $V^{(0),\mathcal{T}^{(m+1)}(F)} \subseteq V^{(0),F}$ is immediate. So, let for the inductive step (side induction) $n+1 > 0$ and assume as inductive hypothesis $V^{(k),\mathcal{T}^{(\ell)}(F)} \subseteq V^{(k\ell),F}$ for all $\langle k, \ell\rangle <_{lex} \langle m+1, n+1\rangle$.

Let $V^{(n+1),\mathcal{T}^{(m+1)}(F)} = V^{(n),\mathcal{T}^{(m+1)}(F)} \cup \{B\}$. Then there exists a functional dependency $(Z \to B) \in \mathcal{T}^{(m+1)}(F)$ such that $Z \subseteq V^{(n),\mathcal{T}^{(m+1)}(F)}$. We can assume that $B \notin V^{(n),\mathcal{T}^{(m+1)}(F)}$ and $(Z \to B) \in \mathcal{T}^{(m+1)}(F) \setminus \mathcal{T}^{(m)}(F)$ since otherwise, the statement follows immediately from the inductive hypothesis. From $m+1 > 1$ we conclude that there exists two functional dependencies $(X \to A), (YA \to B) \in \mathcal{T}^{(m)}(F)$ such that $(XY \to B) \in \mathcal{T}^{(m+1)}(F)$ and $Z = XY$. Since $Z \subseteq V^{(n),\mathcal{T}^{(m+1)}(F)}$ we have $XY \subseteq V^{(n),\mathcal{T}^{(m+1)}(F)}$. From the inductive hypothesis we get $XY \subseteq V^{(n(m+1)),F}$. Hence, A, B can be derived with two loop steps from F and $V^{(n(m+1)),F}$ using the algorithm *transitive closure*. So, we may assume $A, B \in V^{(n(m+1)+2),F}$. From $n(m+1)+2 \leq (n+1)(m+1)$ we get $B \in V^{((n+1)(m+1)),F}$. Hence, $V^{(n+1),\mathcal{T}^{(m+1)}(F)} \subseteq V^{(n+1)(m+1),F}$.

The induction yields $V^{+,tc(F)} \subseteq V^{+,F}$. From $F \subseteq tc(F)$ we conclude $V^{+,tc(F)} = V^{+,F}$. □

Definition 3
Let $R = \langle U, F\rangle$ be a relation schema and $K \in \mathscr{K}_R$. An attribute $A \in U$ is *direct from* K, if there exists a functional dependency $(X \to A) \in F$ such that $X \subseteq K$.

We show in the next proposition that if $A \in U$ is a direct attribute from the key K, then A does not occur in K.

Proposition 4
Let $R = \langle U, F\rangle$ be a relation schema and $K \in \mathscr{K}_R$. If A is direct from K, then $A \notin K$.

Proof. Let $R = \langle U, F\rangle$ be given. Note that F contains only non–trivial unit functional dependencies. Therefore, if $X = K$, then we have immediately $A \notin K$. Thus, we proceed under the assumption $X \subset K$. Let $K \in \mathscr{K}_R$ and $X \to A$ be a functional dependency satisfying $X \subset K$. Suppose that the membership $A \in K$ holds. We set $K' := K - A$. Then $K' \subset K$. We claim, that K' is a superkey of R. From $A \notin X$ and $X \subset K$ we get $X \subseteq K'$, from which we obtain $A \in K'^{+}$. This implies $K'^{+} = K^{+}$. Since K is a key we get $K'^{+} = U$. So, K' is a superkey. But then $K' \not\subset K$ ↯. □

For transitive relation schemas $R = \langle U, F\rangle$ the computation of the transitive closure K^{+} for a key K of R is extremly simple, because the computation process has been "incorporated" into the set F of functional dependencies. This is the statement of the next lemma.

Lemma 5
Let $R = \langle U, F\rangle$ be a transitive relation schema and $K \in \mathscr{K}_R$. Then,

$$K^{+} = K \uplus \{A \in U \mid A \text{ is direct from } K\}.$$

Proof. Let K be a key of R. We consider a computation of K^+ using the algorithm *transitive closure*. We show that the following statement LI is a loop invariant:

$$LI(n) \equiv (Z \to B) \in F \; \& \; Z \subseteq K^{(n)} \; \& \; B \notin K^{(n)} \;\Rightarrow\; \exists (Z' \to B) \in F : Z' \subseteq K.$$

Before entering the while loop in *transitive closure* there is $n = 0$ and $LI(0)$ holds. Assume that $K^{(n)}$ has already been computed and that $LI(n)$ holds. Let $K^{(n+1)} = K^{(n)}A$ and assume that there exists a functional dependency $(Z \to B) \in F$ such that $Z \subseteq K^{(n+1)}$ and $B \notin K^{(n+1)}$.

We show that $LI(n+1)$ holds. Therefore we have to find a functional dependency $(Z' \to B) \in F$, such that $Z' \subseteq K$. In the trivial case $A \in K^{(n)}$ or $Z \subseteq K^{(n)}$ we have nothing to show. So, we procceed under the assumption $A \notin K^{(n)}$ and $Z \not\subseteq K^{(n)}$. Then $A \in Z$ and from $n + 1 > 0$ we conclude that there exists a functional dependency $(X \to A) \in F$ such that $X \subseteq K^{(n)}$. Applying $LI(n)$ to $X \to A$ yields a functional dependency $(X' \to A) \in F$ such that $X' \subseteq K$. Since $Z \subseteq K^{(n+1)} = K^{(n)}A$ and $A \in Z$ we write Z in the form $Z = TA$, where $T = Z - A$. Now, $X'T \subseteq K^{(n)}$ and since R is transitive we have $(X'T \to B) \in F$. We apply $LI(n)$ to $X'T \to B$ and obtain by inductive hypothesis a functional dependency $(Z' \to B) \in F$ such that $Z' \subseteq K$. Hence, $LI(n+1)$ holds. □

The *kernel* I of a set of functional dependencies over the attribute set U is the set of all attributes $A \in U$ which occur only in the left hand side of functional dependencies of F or in trivial functional dependencies of F. Intuitively, the attributes in the kernel are in every key of a relation schema.

Definition 6 (Kernel)
Let F be a set of functional dependencies over the attribute set U. The *kernel* I of F is the following attribute set:

$$I := \{A \in attr(F) \;\big|\; \forall (X \to B) \in F : A \neq B \vee (A \in XB \Rightarrow B \in X)\}.$$

Lemma 7
Let $R = \langle U, F \rangle$ be a relation schema where $U = attr(F)$. Then

$$I \subseteq \bigcap_{K \in \mathscr{K}_R} K.$$

Proof. Let $R = \langle U, F \rangle$ be given. Assume $A \in I$. Then by Definition 6, A occurs only in the left hand side of the functional dependencies in F or in trivial functional dependencies of F. So, in the first case, A cannot be derived from the functional dependencies in F. Since $K^+ = U$ for every $K \in \mathscr{K}_R$, we conclude $A \in \bigcap_{K \in \mathscr{K}_R} K$. In the second case, we have $A \in K^+$ if and only if $A \in K$. Again, $A \in \bigcap_{K \in \mathscr{K}_R} K$. □

3 An Inference System for Deriving Keys

We introduce an inference system $\mathbb{K}$ for deriving keys of a relation schema. Virtually, the entities which are derived with $\mathbb{K}$ are functional dependencies. So, when we speak of deriving a key K we mean to derive a functional dependency $K \to A$.

The system $\mathbb{K}$ is sound in the sense that every functional dependency $X \to A$, which is derived with $\mathbb{K}$, is in F^+. It is complete in the sense that for every key K of a relation schema $R = \langle U, F\rangle$ a functional dependency $K \to A$ is derivable, where $A \in U$ or $A = \varnothing$.

The inference system $\mathbb{K}$ is a Hilbert style inference system. Let $R = \langle U, F\rangle$ be a relation schema. By our convention the functional dependencies in F are non-trivial, unit functional dependencies. The inference system $\mathbb{K}$ depends on R.

Axioms of $\mathbb{K}$

$\varnothing \to \varnothing$

$X \to A \quad$ if $(X \to A) \in F$

Rules of inference of $\mathbb{K}$

$$\mathbb{K}1. \qquad \frac{X \to A \qquad YA \to B}{XY \to B}$$

$$\mathbb{K}2. \qquad \frac{X \to A \qquad Y \to B}{XY \to B}$$

The axioms of $\mathbb{K}$ are essentially the functional dependencies of F. The axiom of the form $\varnothing \to \varnothing$ is only needed when $F = \varnothing$. Then $\varnothing$ is the only key of R. Note that $U = attr(F)$ and so, $F = \varnothing$ implies $U = \varnothing$. Note also, that in the inference rule $\mathbb{K}2$ the two functional dependencies in the premise can be swapped and thus, one can also derive the functional dependency $XY \to A$.

The inference rules of $\mathbb{K}$ have two premises and one conclusion. A derivation $F \vdash_{\mathbb{K}} X \to A$ is defined in the usual way. That is, a derivation $F \vdash_{\mathbb{K}} X \to A$ starts with axioms from $\mathbb{K}$. Then one derives functional dependencies using axioms from $\mathbb{K}$ or functional dependencies which have been derived by previous steps. The length of a derivation $F \vdash_{\mathbb{K}} X \to A$ is defined as the number of inference steps with $\mathbb{K}1$ or $\mathbb{K}2$. The soundness of $\mathbb{K}$ is trivial. So, we address the question of completeness.

Let $R = \langle U, F\rangle$ be a relation schema and $R^+ = \langle U, tc(F)\rangle$ its transitive form. By Lemma 2, the set of keys of R and R^+ coincide. Therefore, we assume in the following considerations that $R = R^+$, that is, R is transitive.

We show how to find non–deterministically a derivation $F \vdash_{\mathbb{K}} K \to A$ of length at most $3|F|$, where K is a key of R and $A \in U$ or $A = \varnothing$. If $F = \varnothing$, then $U = \varnothing$, because by our assumption we have $U = attr(F)$. Then $\varnothing$ is the only key of R. We have $F \vdash_{\mathbb{K}} \varnothing \to \varnothing$ with length zero, because $\varnothing \to \varnothing$ is an axiom of $\mathbb{K}$. We proceed under the assumption $F \neq \varnothing$.

At first we derive a functional dependency $X_1 \to A_1$ using only the inference rule $\mathbb{K}2$. Let $I \subseteq U$ be the kernel of R, and let $\{V_1 \to C_1, \ldots, V_k \to C_k\}$ be a cardinal minimal subset of F such that $V_\kappa \cap I \neq \varnothing$ for all $1 \leq \kappa \leq k$ and $I \subseteq \bigcup_{\kappa=1}^{k} V_\kappa$. Then we derive with $\mathbb{K}2$ the functional dependency $V_1 \ldots V_k \to C_1$. We set $X_1 = V_1 \ldots V_k$ and $A_1 = C_1$. Then we have $F \vdash_{\mathbb{K}} X_1 \to A_1$ and $I \subseteq X_1$. If $X_1 = K$, then we are done. Clearly, this derivation has length at most $|F|$. Otherwise, we make a case analysis.

Case 1: $X_1 - K \neq \varnothing$.
Let $D_1 \in (X_1 - K)$. Since R is a transitive relation schema, by Lemma 5 there exists a functional dependency $Z_1 \to D_1$ in F such that $Z_1 \subseteq K$. Thus, we have the two functional dependencies

$$X_1 \to A_1 \qquad \text{and} \qquad Z_1 \to D_1$$

with the properties

(1) $Z_1 \subseteq K$, and

(2) $|X_1 - K| > |(X_1 - D)Z_1 - K| \geq 0$, because $Z_1 \subseteq K$.

Using the inference rule $\mathbb{K}1$ we obtain

$$[\mathbb{K}1] \qquad \frac{Z_1 \to D_1 \qquad (X_1 - D_1)D_1 \to A_1}{Z_1(X_1 - D_1) \to A_1}$$

If $Z_1(X_1 - D_1) \subseteq K$ holds, then we are ready with case 1. Otherwise, we can apply to $Z_1(X_1 - D_1) \to A_1$ the same consideration as to $X_1 \to A_1$ above. In consideration of (2) we derive after finitely many steps a functional dependency

$$Z_n(\ldots(Z_2(Z_1(X_1 - D_1) - D_2) - \cdots) - D_n) \to A_1$$

such that $Z_n(\ldots(Z_2(Z_1(X_1-D_1)-D_2)-\cdots)-D_n) \subseteq K$. If $Z_n(\ldots(Z_2(Z_1(X_1-D_1)-D_2)-\cdots)-D_n) = K$, then we are done. The length of this derivation is at most $|F|$. Otherwise, there is $Z_n(\ldots(Z_2(Z_1(X_1 - D_1) - D_2) - \cdots) - D_n) \subset K$, and we proceed with case 2. Note that the kernel I fulfills the relation $I \subseteq Z_n(\ldots(Z_2(Z_1(X_1 - D_1) - D_2) - \cdots) - D_n) \subset K$.

Case 2: $X_1 \subset K$.
Then, $X_1^+ \subset U$, because K is a $\subseteq$–minimal key. Let $A_2 \in (U - X_1^+K) \neq \varnothing$. By Lemma 5 there exists a functional dependency $X_2 \to A_2$ in F such that $X_2 \subseteq K$. We have

(1) $X_1X_2 \subseteq K$ by construction, and

(2) $X_1^+ \subset (X_1X_2)^+ \subseteq U$, because $A_2 \in U - X_1^+K$.

Using the inference rule $\mathbb{K}2$ we obtain

$$[\mathbb{K}2] \qquad \frac{X_1 \to A_1 \qquad X_2 \to A_2}{X_1X_2 \to A_2}$$

From (2) we get $|U - X_1^+| > |U - (X_1X_2)^+| \geq 0$. Now, if $(X_1X_2)^+ = U$, then we are done. Otherwise, we can apply to $X_1X_2 \to A_2$ the same consideration as to $X_1 \to A_1$ above, because of (1). Thus, after finitely many steps we can construct a functional dependency $X_1X_2 \dots X_n \to A_n$ such that $|U - (X_1X_2 \dots X_n)^+| = 0$ and $X_1X_2 \dots X_n \subseteq K$. Since K is a key we conclude $X_1X_2 \dots X_n = K$. By construction, we need at most $|F|$ inference steps with $\mathbb{K}2$. Thus, we have proved the following theorem.

Theorem 8
Let $R = \langle U, F \rangle$ be a transitive relation schema. For every key K of R there exists a derivation $F \vdash_{\mathbb{K}} K \to A$, where $A \in U$ or $A = \varnothing$, of length at most $3|F|$. □

Since the set of keys of a relation schema R coincides with the set of keys of its transitive form R^+ by Lemma 2, we get the following completeness theorem for the inference system $\mathbb{K}$.

Theorem 9 (Completeness of $\vdash_{\mathbb{K}}$)
Let $R = \langle U, F \rangle$ be a relation schema. Then, for every key K of R there exists a derivation $F \vdash_{\mathbb{K}} K \to A$, where $A \in U$ or $A = \varnothing$. □

Example 10
Let $R = \langle U, F \rangle$, where $U = \{A, B, C, D, E, F\}$ and

$$F = \{ \begin{array}{rcl} AB & \to & C, \\ DC & \to & E, \\ F & \to & G \,\}. \end{array}$$

The following is a derivation of length 2 of the unique key $ABDF$.

$$[\mathbb{K}2] \quad \frac{[\mathbb{K}1] \quad \dfrac{AB \to C \qquad DC \to E}{ABD \to E} \qquad F \to G}{ABDF \to E} \quad .\lrcorner$$

Example 11
Let $R = \langle U, F \rangle$, where $U = \{A, B, C\}$ and

$$F = \{ \begin{array}{rcl} AB & \to & C, \\ C & \to & B \,\}. \end{array}$$

There are two keys: AB and AC. The derivation of AB has length zero, because the functional dependency $AB \to C$ is an axiom of $\mathbb{K}$.

$$\frac{}{AB \to C}\,.$$

A derivation of AC is given below:

$$[\mathbb{K}1]\ \frac{C \to B \qquad [\mathbb{K}2]\ \dfrac{AB \to C \qquad C \to B}{ABC \to B}}{AC \to B}\quad .\lrcorner$$

Let $R = \langle U, F\rangle$ be a relation schema. We show that the following decision problem is NP–complete: Given a functional dependency $X \to A$; decide whether there is a derivation $F \vdash_{\mathbb{K}} X \to A$ and X is a cardinal minimal key of R. We show at first that this decision problem is in NP. To this end, guess a derivation $F \vdash_{\mathbb{K}} X \to A$ and verify that X is a cardinal minimal key of R. Guessing a derivation can be done in time $\mathcal{O}(|F|)$; note that a (non-deterministic) derivation $F \vdash_{\mathbb{K}} K \to A$ has length $\leq |F|$, because each functional dependency in F must occur at most one time in the derivation. To verify that X is a cardinal minimal key of R we check $X^+ = U$, and we check the inclusion $(X - A)^+ \subset U$ for each $A \in X$. Computing the closure Z^+ of an attribute set Z is polynomial in the input R (cf. [Ullman 1988]). Hence, the verification whether X is a cardinal minimal key of R is polynomial in the input R. Now NP–completeness follows immediately from the fact that finding a cardinal minimal key of a relation schema is NP–complete. See [Lucchesi et al 1978] (or [Garey et al 1979] p. 232, A4.3.1).

Theorem 12
Let $R = \langle U, F\rangle$ be a relation schema. The problem to find a derivation $F \vdash_{\mathbb{K}} K \to A$ such that K is a cardinal minimal key of R is NP–complete.

4 Estimating the Number of Keys

We use the fact that the inference system $\mathbb{K}$ is complete with respect to the set of keys of a relation schema.

Theorem 13
Let $R = \langle U, F\rangle$ be a relation schema such that F is a set of non-trivial unit functional dependencies. Then, R has at most $\lfloor e^{|F|/e} \rfloor$ keys.

Proof. Let $R = \langle U, F\rangle$ be given. We define a graph structure in order to estimate the number of keys of R. The digraph $\mathscr{G} = \langle V, E\rangle$ has vertex set

$$V = F$$

and edge set

$$E = \{(X \to A) \longrightarrow (YA \to B) \bigm| (X \to A), (YA \to B) \in F\}.$$

Let $C_1, \ldots, C_k \subseteq V$ be the strongly connected components of $\mathscr{G}$. Now in the most optimistic case every left hand side of a vertex in a strongly connected component is a key of that component. So, we can estimate the number of keys of R by

$$|\mathscr{K}_R| \leq |C_1| \cdots |C_k|.$$

Note that the effect of the inference rule $\mathbb{K}2$ is implicit in the product $|C_1| \cdots |C_k|$. We show that if every strongly connected component C_κ has $\frac{|F|}{k}$ elements, then the product $|C_1| \cdots |C_k|$ will be maximal.

<u>Claim:</u> $\forall k \geq 1$: if every C_κ $(1 \leq \kappa \leq k)$ has $\frac{|F|}{k}$ elements, then the product $|C_1| \cdots |C_k|$ is maximal.

Proof. We solve the following extremal problem using the Lagrange multiplier method (cf. [Edwards 1973]). Let $N = |F|$. Determine the maximum of the function

$$f : \begin{cases} \mathbb{R}^k \to \mathbb{R} \\ \langle x_1, x_2, \ldots, x_k \rangle \mapsto x_1 x_2 \cdots x_k \end{cases}$$

subject to $x_1 + x_2 + \cdots + x_k = N$ on the k–dimensional interval $I = [1, N]^k \subseteq \mathbb{R}^k$. Let $g(x_1, x_2, \ldots, x_k) = x_1 + x_2 + \cdots + x_k - N$. We solve the following system of $k+1$ equations in the $k+1$ indeterminates $x_1, x_2, \ldots, x_k, \lambda$.

$$\begin{aligned} g(x_1, x_2, \ldots, x_k) &= 0 && (1) \\ \nabla f(x_1, x_2, \ldots, x_k) &= \lambda \nabla g(x_1, x_2, \ldots, x_k). && (2) \end{aligned}$$

This yields

$$\begin{aligned} x_1 + x_2 + \cdots + x_k - N &= 0 && (3) \\ x_1 \cdots x_{i-1} x_{i+1} \cdots x_k &= \lambda \qquad (1 \leq i \leq k) && (4) \end{aligned}$$

Multiplying (3) with λ in consideration with (4) yields

$$k x_1 x_2 \cdots x_k = \lambda N,$$

from which we get $\lambda = \frac{k x_1 x_2 \cdots x_k}{N}$. With (4) we obtain

$$x_i = \frac{N}{k} \qquad (1 \leq i \leq k).$$

Finally, we verify the uniqueness of this solution. Suppose that $r_1, r_2, \ldots, r_k, \lambda' \in \mathbb{R}$ is another solution of (3) and (4). Then from (3) and (4) we get $k r_1 r_2 \cdots r_k = \lambda' N$ and further, $r_i = \frac{N}{k}$ for all $1 \leq i \leq k$. Hence, $x_i = r_i$ for all $1 \leq i \leq k$. $\square$

From the claim we get

$$|\mathscr{K}_R| \leq \lfloor \underbrace{\frac{|F|}{k} \cdots \frac{|F|}{k}}_{k \text{ factors}} \rfloor .$$

Let $N = |F|$. We investigate the real valued function $\varphi : x \mapsto \frac{N^x}{x^x}$ on the intervall $[1, N] \subseteq \mathbb{R}$, where $N \in \mathbb{N}$ and $N \geq 3$. We determine the maximum of φ in the intervall $[1, N]$. Therefore we compute the zeros of the derivative φ':

$$N^x x^{-x}(\ln N - \ln x - 1) = 0.$$

Since $N^x x^{-x}$ is always positive on $[1, N]$, we consider

$$\ln N - \ln x - 1 = 0.$$

This yields the zero $x = \frac{N}{e}$ which is the only extremal point in $[1, N]$. Now if $|F| < 3$, then R has at most 2 keys. Hence we get $|\mathscr{K}_R| \leq \lfloor e^{|F|/e} \rfloor$. □

It is easy to construct an example of a relation schema such that $|\mathscr{K}_R| = |C_1| \cdots |C_k|$.

Example 14
Consider the set F of functional dependencies

$$\begin{aligned} F \;=\; \{ & A_1^1 \to A_1^2, A_1^2 \to A_1^3, \ldots, A_1^{k_1-1} \to A_1^{k_1}, A_1^{k_1} \to A_1^1, \\ & A_2^1 \to A_2^2, A_2^2 \to A_2^3, \ldots, A_2^{k_2-1} \to A_2^{k_2}, A_2^{k_2} \to A_2^1, \\ & \vdots \\ & A_n^1 \to A_n^2, A_n^2 \to A_n^3, \ldots, A_n^{k_n-1} \to A_n^{k_n}, A_n^{k_n} \to A_n^1 \}. \end{aligned}$$

Then

$$\mathscr{K}_R = \{A_1^1, \ldots, A_1^{k_1}\} \times \{A_2^1, \ldots, A_2^{k_2}\} \times \cdots \times \{A_n^1, \ldots, A_n^{k_n}\} \leq e^{|F|/e}.$$

Related Work

In [Thalheim 1992] it is shown that the number of keys of a relation schema is bounded by $\binom{n}{\lfloor \frac{n}{2} \rfloor}$, where $n = |U|$. Note that this estimation depends on U, whereas our estimation depends on F. This is an essential difference. Below, we estimate the number of keys for small powers of 2. We consider the cases $|F| = 0.75 \cdot |U|$, $|F| = |U|$ and $|F| = 1.25 \cdot |U|$. Notice that the assumption $|F| = 1.25 \cdot |U|$ is very pessimistic.

n	$\binom{n}{\lfloor \frac{n}{2} \rfloor}$	$\lfloor e^{3n/4e} \rfloor$	$\lfloor e^{n/e} \rfloor$	$\lfloor e^{5n/4e} \rfloor$
2	2	1	2	2
4	6	3	4	6
8	70	9	18	39
16	12870	82	359	1568
32	$\sim 6 \cdot 10^8$	6830	129 591	2 458 784

5 Conclusions

We have introduced an inference system $\mathbb{K}$ for deriving (non–deterministically) all keys of a relation schema. The problem to find a derivation $F \vdash_{\mathbb{K}} X \to A$ such that X is a cardinal minimal key is NP–complete. Then we have estimated the number of keys of a relation schema $R = \langle U, F \rangle$ by $\lfloor e^{|F|/e} \rfloor$.

References

[Armstrong 1974] Armstrong, W.W.: "Dependency Structures of Data Base Relationships"; Proceedings of the IFIP Congress 1974, 580–583.

[Edwards 1973] Edwards, Jr., C.H.: "Advanced Calculus of Several Variables"; Academic Press (1973).

[Garey et al 1979] Garey, M.R., Johnson, D.S.: "Computers and Intractability"; W.H. Freeman and Company (1979).

[Lucchesi et al 1978] C.L. Lucchesi, C.L., Osborn, S.L.: "Candidate Keys for Relations"; JCSS (Journal of Computer and System Sciences), 17, (1978), 270–279.

[Maier 1983] Maier, D.: "The Theory of Relational Databases"; Computer Science Press (1983).

[Mendelson 1987] Mendelson, E.: "An Introduction to Mathematical Logic"; Wadsworth & Brooks/Cole Advandced Books and Software, third edition (1987).

[Thalheim 1992] B. Thalheim. On the number of keys in relational and nested relational databases. *Discrete Applied Mathematics*, 40(265-282), 1992.

[Ullman 1988] Ullman, J.D.: "Principles of Databases and Knowledge Bases, Vol. 1"; Computer Science Press (1988).