KYBERNETIKA — VOLUME 9 (1973), NUMBER 6

Contributions to Automatic Construction and Optimalization of Identification Keys

KAMILA BENDOVÁ

In this paper an attempt is made to give a mathematical description of an identification key with special regard to keys in current use in biology. Such mathematical object is to serve for the study of problems in constructing keys and of criteria for their evaluation and mutual comparison. The aim of the study is to discover possibilities for developing algorithms on the basis of which a computer could construct suitable keys or improve those already established.

The present problem may be consider as a part of an extensive complex of questions involving various aspects relating to classification (i.e. mapping, distribution) in the broadest sense of the term. A mathematical solution of these problems becomes indispensable for science, technology and economic coordination. The practical results in the construction of biological identification keys would with small modifications be applicable in various other fields, such as economical catalogization, accelerated sorting of data, efficient storage and distribution.

In view of the possible applications it is useful, before attempting the mathematical description, to state what an identification key is and what can reasonably be expected from it in order to avoid possible misunderstanding and confusion with seemingly alike structures. Hierarchical classification will be mentioned in the following mainly for the purpose of stressing differences in concepts. In other respects the comments do not claim either precision or completeness.

The basic difference between a hierarchical classification and an identification key is evident if only intuitively to any scientic worker, at least in biology where both systems are in current use. However, this intuition fails when we have to construct and to suggest a mathematical description of artificial systems (i.e. hierarchical classifications and identification keys) which in substance means following certain criteria chosen beforehand. Confusion in viewpoints and requirements, lack of precision of the criteria as well as erroneous interpretation of the results often lead to a sceptical attitude among biologists.

Therefore, we shall briefly state what is understood in science in general and in biology in particular by the concepts of hierarchical classifications and identification keys, what basic requirements need be fulfilled and what are the normal criteria of their suitability.

Hierarchical classification is a means for structuring and ordering our knowledge. Its objective is to arrange some beforehand defined empirical (i.e.potentially open or infinite) set of objects, i.e. the animal kingdom, into a system with descending hierarchy in such a way that any object is uniquely fixable at whatever hierarchical level and that its position on one level uniquely determines its place on all higher levels. Mathematically speaking each level represents the covering of the whole set by pairwise disjoint subsets. On the hierarchically highest level the covering consists of one element only. The levels are linearly ordered, each set of this system is either included in the set on a higher level or is disjoint with it.

The arrangment into subsets is done on the basis of a defined set of properties. However, and this is significant for a hierarchical classification, allocation to the corresponding set is not necessarily bound to the presence of a property or a group of properties. The determinant criterion of classification is the high degree of similarity between the elements of the same sets. "Similarity" being a subjective criterion is difficult to describe in exact terms; sufficient to say that the degree of similarity is given by the whole set and that some sets need not be defined explicitly but only as classes grouping elements of similar nature.

A hierarchical classification already implicitly supposes a concept of that knowledge for which hierarchization is done. In order to allow at all investigation of the intuitively estimated degree of similarity a group of preferred properties has to be separated and it must be decided which attributes are fundamental in respect of a given concept (e.g. evolution theory) and which are secondary. In judging hierarchical classifications the aspect of economy is subsidiary to the requirement that all corresponding subsets (and associated concepts) of the same hierarchical type be on one hierarchical level. From a purely formal point of view, one may speak of a tendency to place all the minimal subsets (e.g. species) of a system (or at least large subsystems) of a hierarchical classification on the same level.

Two characteristic features of a hierarchical classification are connected with the foregoing statement. One is the admissibility of a hierarchically higher concept (or a whole series of them) containing a single lower concept. The other feature is the admissibility and virtually almost inevitability of a nondyadic division. A hierarchical classification generally is not regarded as a means, a merely technical tool, but rather as the result and essential component of a complex and long-lasting process of cognition. Direct allocation of a particular object on a higher hierarchical level might be an entirely nontrivial achievement which takes into the consideration the interrelationship of the whole system and requires technically demanding and thorough investigation of the given object (e.g. study of discrete phase of ontogenesis). In practice this is not done since, as already known, for unique allocation of an object in the whole system of the hierarchical classification it is sufficient to place it on the lowest hierarchical level (in biology this means assignement to a particular species). It is only on this hierarchical level where each subset has to be fully determined by a specific combination of properties (conjunction of properties or of their negations), in other words that any object be clearly and independently identifiable and, if possible, in a mechanical and simple manner.

An identification key is the very instrument for this purpose. It prescribes a mechanical procedures which applied to any object leads to its identification, i.e. assigns to it just one species (subset). The identification key is secondary in the sense that it assumes an already existing hierarchical classification (or generally any classification) of a given empirical complex, in other words a system of subsets (OTU's – operational taxonomic units, in biology corresponding species) presenting a disjointed covering of the whole complex with a finite set of properties by which this covering can be fully defined. Whenever in the following, for the sake of briefness, "species" is mentioned, it means the corresponding subset of the covering determined by the characteristic function which is defined on the given set of properties, i.e. for each property it is true that all elements of the subset have this property or all elements of the subset do not have this property. In the identification of an unknown object it would be highly impractical but in principle possible to investigate first the course of the characteristic function and then to go through the list of species until the respective species with the same characteristic function is found. The identification key operates according to the following principle: If an element has or has not a certain property the list of relevant species is reduced. For such a reduced list we chose another property which divides the list again. Finally, only one species is left – the one we were looking for. It can be seen that the identification key divides the given complex in a similar manner as a hierarchical classification. The result is a hierarchical system ending in the same subsets (species) allowing to identify through such steps any unknown object in terms of the species. This morphological similarity precisely is the source of confusion. However, the two types of division substantially differ both in the objectives and requirements. Instead of proper hierarchization in the sense of a given concept of knowledge the aim of identification key is the fast identification of an unknown object. Properties therefore are not judged by their "importance" but by their "suitability" for division. Furthermore the individual identification steps have to be independent of each other, i.e. each subset of the system must uniquely be defined by the relevant properties contrary to hierarchical classification where similarity classes occur. This implies (again in contrast to hierarchical classification) that each identification key can be transformed into a dyadic one. Finally, it is clear, that, for the sake of economy, ineffective steps are to be avoided. Consequently, it is not necessary that the species occur on the same level.

In summarizing the above comments it can be stated that, notwithstanding the analogy between the two systems, natural hierarchical classification (and in certain aspects also "artificial" one) represents some sort of compendium of our knowledge about the given complex of objects. On the other hand, a key is a mere technical means for a fast and reliable orientation in this compendium. As one cannot dispense of the source document in compiling a register, so thus one need beforehand a hierarchical classification for the construction of an identification key. On the contrary, a key like a register follows, in subdividing and sorting out the given material, completely different criteria. A hierarchical classification assigns to the object a system of sets which clarify its nature and its place in the complex; a key assigns to it a certain sequence of steps aligning it with identical (in the sense of classification) objects. It should be added that our choice of terminology is adjusted to the purely auxiliary character of the system.

These problems were discussed in greater detail in order to avoid misunderstanding as well as to elucidate the merits of the criteria applied to the material. Criteria of "economy" were on purpose not specified as their precise formulation is an essential part of the present work. Here it should only be mentioned that contrary to the current biologist's concept certain restrictions were adopted beforehand in the formulation of the problem. In the first place only dyadic keys will be considered. Owing to the convertibility of all keys into dyadic ones, already mentioned above, most of the results obtained can in principle be applied also to nondyadic keys. Furthermore no attention will be paid to differences in the frequency of occurrence of a given species or to the difficulties in examining individual properties.

This work is divided into two parts: the first deals with mathematical description of a key, formulation of criteria for comparison and some partial results concerning the error of a partition. At the end of the first part, it will be shown what are the possibilities for the key construction. In the second part a possible method applicable in the automatic construction and optimalization of keys is suggested.

The present work belongs to the field of problems dealt with on the seminar about the applications of mathematical logic on the Mathematico-physical faculty of Charles University in years 1970–71. I should like to present my thanks to all the participants for the many suggestions and useful criticism which substantially helped to put this paper into the present form. Above all I express my profound gratitude to Dr Petr Hájek the leader of the seminar on whose iniciative this investigation was started for his outstanding help, continuous encouragement and support.

1. NOTATION

In this section we shall summarize some known notions from logic and the theory of partially ordered sets useful for our purpose.

A language consists of (1) unary predicate symbols $P_1, \ldots, P_n$, (2) one individual variable (which can, for shortness, be ommited), (3) logical connectives and (4) quantifiers.

We adopt the usual notion of formulas, $\bigwedge_{i=1}^{0} \varepsilon_i \times P_i$ – an empty conjunction – is also a formula. Thus an *elementary conjunction* is each formula $\bigwedge_{i=1}^{k} \varepsilon_i \times P_i$ where $\varepsilon_i \in \{0, 1\}$, $0 \times P = \neg P$, $1 \times P = P$ and $k \geqq 0$.

A *model* (semantic unary model of the type n) is a finite non-empty set E and n predicates $\mathscr{P}_1, \ldots, \mathscr{P}_n$ (properties). We write $\mathscr{M} = \langle E, \mathscr{P}_1, \ldots, \mathscr{P}_n \rangle$. We can also assign to each predicate $\mathscr{P}_i$ a function v_i mapping E into the two-elements set $\{0, 1\}$ such that $v_i(e) = 1$ if $\mathscr{P}_i(e)$ and $v_i(e) = 0$ if non $\mathscr{P}_i(e)$ for each $e \in E$. Then we mean by a model $\mathscr{M}$ the set E with the functions $v_1, \ldots, v_n$.

The satisfaction is defined as usual; in our particular case an elementary conjunction $\bigwedge_{i=1}^{k} \varepsilon_i \times P_i$ is satisfied by e in $\mathscr{M}$ (we write $\mathscr{M} \vdash \bigwedge_{i=1}^{k} \varepsilon_i \times P_i[e]$) if $\mathscr{P}_i(e)$ as soon as $\varepsilon_i = 1$ and non $\mathscr{P}_i(e)$ as soon as $\varepsilon_i = 0$.

1.1. Definition. A *tree* is a partially ordered set $(V, \leqq)$ with the following properties:

1) V is finite and non-empty;

2) $(\forall x \in V)(\{y; y \leqq x\}$ is linearly ordered);

3) $(\exists z \in V)(\forall x \in V)(z \leqq x)$.

Remark. By 3) there is a least element; it will be called the root k_V.

1.2. Definition. We say that a tree V is a *dyadic tree* if

$$(\forall x \in V)(x \neq k_V \Rightarrow (\exists!\, y \in V)(x \parallel y \;\&\; \{z; z < x\} = \{w; w < y\}))\,.$$

1.3. Definition. The *canonical tree* $(U, \leqq)$ is a set of all finite sequences of zeros and ones with the natural partial ordering of sequences:

$$\langle a_1, \ldots, a_k \rangle, \langle b_1, \ldots, b_l \rangle \in U \Rightarrow$$
$$\Rightarrow (\langle a_1, \ldots, a_k \rangle \leqq \langle b_1, \ldots, b_l \rangle \equiv k \leqq l \;\&\; (\forall i \leqq k)(a_i = b_i))\,.$$

Remark. Let $(U, \leqq)$ be the canonical tree and let $V \subseteq U$. We shall always suppose that V is partially ordered by the natural partial ordering.

1.4. Definition. Let $(U, \leqq)$ be the canonical tree, $a = \langle a_1, \ldots, a_k \rangle$, $b = \langle b_1, \ldots, b_l \rangle$. We define:

1) the *composition* $a * b = \langle a_1, \ldots, a_k, b_1, \ldots, b_l \rangle$ (in particular, we write $a * 0 = a * \langle 0 \rangle = \langle a_1, \ldots, a_k, 0 \rangle$, $a * 1 = a * \langle 1 \rangle = \langle a_1, \ldots, a_k, 1 \rangle$);

2) the *meet* $a \wedge b = \langle c_1, \ldots, c_h \rangle$ if $a = \langle c_1, \ldots, c_h, a_{h+1}, \ldots, a_k \rangle$ & $b = \langle c_1, \ldots, c_h, b_{h+1}, \ldots, b_l \rangle$ & $a_{h+1} \neq b_{h+1}$.

3) the function *next*: if $a < b$ i.e. $b = \langle a_1, \ldots, a_k, b_{k+1}, \ldots, b_l \rangle$ then next $(a, b) = b_{k+1}$.

We call

a) $\emptyset$ the *root* (obviously $\emptyset$ is the least element);

b) $a * 0$, $a * 1$ the *successors* of a;

c) $Pr(a) = \langle a_1, \ldots, a_{k-1} \rangle$ the *predecessor* of a;

d) $d(a) = \langle a_1, \ldots, a_{k-1}, \bar{a}_k \rangle$ where $\bar{0} = 1$ and $\bar{1} = 0$ the *neighbour* of a;

e) $|a|$ the *norm* of a if $a = \langle a_1, \ldots, a_{|a|} \rangle$.

1.5. Definition. Let $(U, \leqq)$ be the canonical tree. We say that $V \subseteq U$ is a *segment of the canonical tree* if

1) V is a finite and non-empty subset of U;

2) $(\forall x \in V)(\forall y \in U)(y < x \rightarrow y \in V)$;

3) $(\forall x \in V)(x \neq \emptyset \rightarrow d(x) \in V)$.

Remark. A segment of the canonical tree is obviously a dyadic tree.

1.6. Lemma. Every dyadic tree is isomorphic to some segment of a canonical tree.

By the term dyadic tree we understand in the following a segment of a canonical tree.

Remark. Let V be a dyadic tree. Then elements of V (i.e. vertices of the canonical tree) are of two kinds:

1) Vertices $u \in V$ such that $u * 0 \in V$ and $u * 1 \in V$. We call them *nodes* of V;

2) vertices $u \in V$ such that $u * 0 \notin V$ and $u * 1 \notin V$. We call them *vertices* of V and we denote the set of all vertices of V by $\mathbf{V}(V)$.

2. KEYS AND CRITERIA — DEFINITIONS

The problem presented in this section deals with a mathematical description of identification key as particularly known in biology. To the biologist a key represents a book with an organized system of questions and references arranged in chains each terminated in the taxon (name of OTU – operational taxonomic unit) identifying the individual. The answer to a question refers to another question; each taxon has its own sequence or, in other words, only one sequence of answers corresponds to a particular taxon.

The dyadic key with its questions and two references to another question is similar to a dyadic tree where questions are assigned to nodes and references to edges.

Before constructing a key a complex of individuals, a set of taxons (OTU's) and a set of properties must be given. The individuals of the same taxon are identical with respect to the set of properties, and two individuals of different taxons are discernible by some property (from our set). We shall therefore consider only a set which contains one representant of each taxon. Our original aim will be achieved if we succeed in the construction of a key distinguishing all elements of this representative set.

Let us have a set E of objects and a sequence of properties (predicates) $\mathscr{P}_1, \ldots, \mathscr{P}_n$.

This forms a model $M = \langle E, \mathscr{P}_1, \ldots, \mathscr{P}_n \rangle$ such that objects of E are discernible in the sense of $\mathscr{M}$, i.e. if for $e_1, e_2 \in E$ is $e_1 \neq e_2$ then there is a $\mathscr{P}_j$ such that $\mathscr{M} \vdash P_j[e_1]$ iff $\mathscr{M} \vdash \neg P_j[e_2]$. In the following, we will always use the letter $\mathscr{M}$ for a model $\mathscr{M} = \langle E, \mathscr{P}_1, \ldots, \mathscr{P}_n \rangle$.

2.1. Definition. Let $(U, \leqq)$ be the canonical tree and let $V \subseteq U$. Then $\overline{V} = V \cup \{u \in U; (\exists v \in V)\, (v = Pr(u))\}$ is called the *completion* of V.

2.2. Definition. f is a *tree-function* if $\overline{\mathbf{D}}(f)$ $(= \overline{\mathbf{D}(f)})$ is a dyadic tree.

We denote the set of vertices of $\overline{\mathbf{D}}(f)$ to $\mathbf{V}(f)$. $\mathbf{D}(f)$ is the set of nodes of $\overline{\mathbf{D}}(f)$.

2.3. Definition. Let f be a tree-function into the set of predicate symbols and let $\mathscr{M}$ be a model. Then for $u \in \overline{\mathbf{D}}(f)$ we define:

1) the conjunction corresponding to the node u and to the function f:

$$k(u) = \bigwedge_{v < u} \operatorname{next}(v, u) \times f(v)$$

where $0 \times P = \neg P$, $1 \times P = P$,

2) the set of objects of $A \subseteq E$ by which the respective conjunction is satisfied in $\mathscr{M}$:

$$A_u^f = \{e \in A;\ \mathscr{M} \vdash k(u)\,[e]\}\,,$$

3) the system of subsets of f determined by the respective conjunctions:

$$A_f = \{A_u^f;\ u \in \overline{\mathbf{D}}(f)\}\,.$$

2.4. Definition. A tree-function f is a *key* for $A \subseteq E$ on $\mathscr{M}$ if

1) $\operatorname{card}(A) > 1$,

2) $(\forall u \in \overline{\mathbf{D}}(f))\, (A_u^f \neq \emptyset)$,

3) $(\forall e \in A)\, (\exists u \in \overline{\mathbf{D}}(f))\, (A_u^f = \{e\})$,

f is a *partial key* for $A \subseteq E$ on $\mathscr{M}$ if f satisfies the conditions 1), 2).

Remark. If f is a key then clearly $k(u)$ is an elementary conjuction for every $u \in \overline{\mathbf{D}}(f)$.

2.5. Lemma. Let f be a partial key for $A \subseteq E$ on $\mathscr{M}$. Then

$$(\forall e \in E)\, (\exists!\, u \in \mathbf{V}(f))\, (e \in E_u^f)\,.$$

Proof. First we prove that for every partial key on $\mathscr{M}$ we have $\mathscr{M} \vdash \bigvee_{u \in \mathbf{V}(f)} k(u)$. Let $\mathbf{D}(n) = \bigvee\{k(u),\ (u \in \mathbf{D}(f)\ \&\ |u| = n) \vee (u \in \mathbf{V}(f)\ \&\ |u| \leqq n)\}$. By induction using the equivalence $(\varphi\ \&\ \neg P) \vee (\varphi\ \&\ P) \equiv \varphi$ it is easy to show that $\mathscr{M} \vdash D(n)$ for every $\mathscr{M}$ and every n. For $n > \max_{u \in \mathbf{D}(f)} |u|$ it follows $\mathscr{M} \vdash \bigvee_{u \in \mathbf{V}(f)} k(u)$ thus $(\forall e)\, (\exists u)$.

$.(u \in \mathbf{V}(f)\ \&\ e \in E_u^f)$. Let $u_1 \neq u_2$ be two vertices such that $e \in E_{u_1}^f$ and $e \in E_{u_2}^f$ i.e. $\mathcal{M} \vdash k(u_1)[e]$, $\mathcal{M} \vdash k(u_2)[e]$. Clearly next $(u_1 \wedge u_2, u_1) \neq$ next $(u_1 \wedge u_2, u_2)$ hence

$$\mathcal{M} \vdash (\text{next}\,(u_1 \wedge u_2, u_1) \times f(u_1 \wedge u_2) \not\equiv \text{next}\,(u_1 \wedge u_2, u_2) \times f(u_1 \wedge u_2))\,[e]$$

which is a contradiction.

The book where the key f is written in some appropriate ordering is exactly the key in the biologist's sense. If we return to this original conception then for comparing keys – with the restrictions accepted above – three demands can be stressed:

1) the extend of the book;
2) the average number of steps which is necessary for identification;
3) the maximal number of steps which is necessary for identification.

We shall investigate how we can express these demands in the frame of our formalization; if we can use them as criteria of suitability and which form of domain (resp. $\bar{\mathbf{D}}(f)$) must be assumed for f to be a suitable key, i.e. minimal in the sense of some one from the above criteria.

2.6. Denotation. $\mathcal{S}_n$ is the class of all trees with n vertices.

Let $\mathcal{M}$ be a model, card $(E) = n$, f a key for E. Then clearly $\bar{\mathbf{D}}(f)$ is an element of $\mathcal{S}_n$.

2.7. Lemma. Let $Z \in \mathcal{S}_n$, let $p(Z)$ be the number of nodes in the tree Z. Then $p(Z) = n - 1$.

Thus $p(\bar{\mathbf{D}}(f))$ which corresponds to the extend of a book is constant. This is implied already by the definition of a key. So we cannot consider it as a criterion of suitability.

2.8. Definition. Let $Z \in \mathcal{S}_n$, $s(Z) = \sum_{u \in \mathbf{V}(Z)} |u|$. Then we define a *criterion* s:

$$Y, Z \in \mathcal{S}_n \Rightarrow (Y \leqq_s Z \equiv s(Y) \leqq s(Z))\,.$$

Remark. The criterion s is obviously a partial quasi-ordering on $\mathcal{S}_n$.

2.9. Theorem. The following three statements are equivalent:

1) $Z \in \mathcal{S}_n$ is minimal in $\mathcal{S}_n$ in the sense of s,

2) the vertices of Z are on the levels k and $k + 1$ where $k = [\log_2 n]$ (we put $L_2(n) = [\log_2 n]$),

3) $s(Z) = n(L_2(n) + 2) - 2^{L_2(n)+1}$.

2.10. Theorem. The following three statements are equivalent:

1) $Z \in \mathcal{S}_n$ is maximal in $\mathcal{S}_n$ in the sense of s,

2) for every node u of Z it holds: $u * 0$ is a vertex or $u * 1$ is a vertex,
3) $s(Z) = \frac{1}{2}(n^2 + n - 2)$.

Remark. The results of 2.9 and 2.10 are known, see [2] (the question of minimal trees is solved less generally by finding one minimal tree).

2.11. Definition. Let $Z \in \mathscr{S}_n$, $d(Z) = \max_{u \in V(Z)} |u|$. Then we define a *criterion* d:

$$Y, Z \in \mathscr{S}_n \Rightarrow (Y \leqq_d Z \equiv d(Y) \leqq d(Z)) .$$

Remark. The criterion d is obviously a partial quasi-ordering on $\mathscr{S}_n$. The minimal and maximal trees in the sense of d are the same as these in the sense of s but in general these criteria are different.

Thus we can consider both s which corresponds to the average number of steps and d which corresponds to the maximal number of steps as criteria of suitability. In the following we restrict ourselves to the criterion s. If we use terms good, better etc. we will mean good, better etc. in the sense of the criterion s.

3. THE THEORY OF ERROR

By Theorem 2.9 we know the best trees in the sense of criterion s. It is possible that in the model no key f exists the $\bar{\mathbf{D}}(f)$ of which is one of the best trees. Hence we shall try to find an optimal key on $\mathscr{M}$, i.e. a key f such that $\bar{\mathbf{D}}(f)$ is optimal among all trees $\bar{\mathbf{D}}(g)$ where g is a key.

For this purpose we answer two other questions:

1) Let $\mathscr{M}$ be a model; we are constructing a key on $\mathscr{M}$ from the root and we have already a partial key f. Can we say something about f with respect to any key $\bar{f}$ which is an extension (i.e. $\bar{f} \upharpoonright \mathbf{D}(f) = f$) of f?

2) Theorem 2.9 gives the conditions for a tree to be optimal. How are the conditions for a function f such that $\bar{\mathbf{D}}(f)$ is optimal?

3.1. Definition. Put $z(n) = n(L_2(n) + 2) - 2^{L_2(n)+1}$ where $L_2(n) = [\log_2 n]$ and

$$er(a, b) = z(a) + z(b) + a + b - z(a + b) .$$

We call $er(a, b)$ the *error of a partition.*

Remark. By Theorem 2.9 $z(n)$ is $s(Z)$ if $Z \in \mathscr{S}_n$ is the best key. The error of a partition in the root $er(\text{card}\,(E_0^f), \text{card}\,(E_1^f))$ is thus the difference between $s(\bar{\mathbf{D}}(g))$ and $s(\bar{\mathbf{D}}(f))$ where f is a key which after deviding to the subsets E_0^f, E_1^f is best devided and g is a key which is best devided already from the root.

3.2. Theorem. Let $a, b \in N$. The function er has the following properties:
A. $er(a, b) = er(b, a)$.

B. $er(a + 1, b - 1) = er(a, b) + L_2(a) - L_2(b - 1)$.

C. $er(a - [a/2], [a/2]) = 0$.

D. $er(a, b) \geqq 0$.

E. for every model $\mathcal{M}$ where card $(E) = n$ and every key f for E on $\mathcal{M}$ we have the following:

$$s(f) = s(\bar{\mathbf{D}}(f)) = z(n) + \sum_{u \in \mathbf{D}(f)} er(\text{card}(E^f_{u*0}), \text{card}\,(E^f_{u*1}))\,.$$

Proof. A. Obvious.

B. First we prove $z(n + 1) = z(n) + L_2(n) + 2$.

1) Let $L_2(n + 1) = L_2(n)$; then

$$z(n + 1) = (n + 1)(L_2(n) + 2) - 2^{L_2(n)+1} = z(n) + L_2(n) + 2\,.$$

2) Let $L_2(n + 1) = L_2(n) + 1$, i.e. $n + 1 = 2^{L_2(n)+1}$ then $z(n + 1) = (n + 1)\,.$ $.\,(L_2(n) + 3) - 2^{L_2(n)+2} = z(n) + L_2(n) + 2$.

Thus we have $z(a + 1) = z(a) + L_2(a) + 2$, $z(b - 1) = z(b) - L_2(b - 1) - 2$ and hence $er(a + 1, \; b - 1) = z(a + 1) + z(b -- 1) + a + b - z(a + b) =$ $= er(a, b) + L_2(a) - L_2(b - 1)$.

C. 1) Let $L_2([a/2]) = L_2(a - [a/2]) = L_2(a) - 1$. Then $er([a/2], a - [a/2]) =$ $= [a/2]\,(L_2(a) + 1) - 2^{L_2(a)} + (a - [a/2])\,(L_2(a) + 1) - 2^{L_2(a)} + a - a(L_2(a) +$ $+ 2) + 2^{L_2(a)+1} = 0$.

2) Let $L_2([a/2]) = L_2(a) - 1$ and $L_2(a - [a/2]) = L_2(a)$. The proof is similar.

D. First we prove: If $a \geqq b$ then $er(a + 1, \; b - 1) \geqq er(a, b)$. Since $a \geqq b$ it follows that $L_2(a) - L_2(b - 1) \geqq 0$ and thus $er(a + 1, \; b - 1) = er(a, b) +$ $+ L_2(a) - L_2(b - 1) \geqq er(a, b)$.

Let $a > b$. We construct two sequences $\{a_i\}^n_{i=1}, \{b_i\}^n_{i=1}$: $a_1 = a, a_{i+1} = a_i - 1$, $a_n = a + b - [(a + b)/2]$, $b_1 = b$, $b_{i+1} = b_i + 1$, $b_n = [(a + b)/2]$. Then $er(a_n, b_n) = 0$ and clearly $a_i \geqq b_i$ for $i = 1, \ldots, n$. Thus $er(a, b) \geqq er(a_1, b_1) \geqq \ldots \geqq$ $\geqq er(a_n, b_n) = 0$.

E. Let f be a key, $u \in \mathbf{D}(f)$. We denote by f^u the following function: $\mathbf{D}(f^u) =$ $= \{w; u * w \in \mathbf{D}(f)\}$ and for $w \in \mathbf{D}(f^u)$ is $f^u(w) = f(u * w)$. f^u is clearly a key for E^f_u and we have $(E^f_u)^{f^u}_w = E^f_{u*w}$. The *norm of f* is defined as follows:

$$|f| = s(f) - z(\text{card}\,(E)) = \sum_{u \in \mathbf{V}(f)} |u| - z(\text{card}\,(E))\,.$$

First we prove the following Lemma: Let f be a key for E. If we write $er_f(u) =$ $= er(\text{card}\,(E^f_{u*0}), \text{card}\,(E^f_{u*1}))$ then

$$|f| = |f^0| + |f^1| + er_f(\emptyset)\,.$$

Let card $(E) = n$.

1) Let card $(E_0^f) = 1$. Then

$$s(f) = \sum_{u \in \mathbf{V}(f)} |u| = 1 + \sum_{\substack{u \in \mathbf{V}(f) \\ u \geqq 1}} |u| = 1 + s(f^1) + n - 1 = n + s(f^1)$$

hence

$$|f| = s(f) - z(n) = n + s(f^1) - z(n-1) - z(1) + \mathrm{er}(n-1, 1) - n = \\ = |f^1| + er_f(\emptyset)\,.$$

2) Let card $(E_1^f) = 1$. The proof is similar.
3) Let card $(E_0^f) > 1$ and card $(E_1^f) > 1$. Then

$$s(f) = \sum_{u \in \mathbf{V}(f)} |u| = \sum_{\substack{u \in \mathbf{V}(f) \\ u \geqq 0}} |u| + \sum_{\substack{u \in \mathbf{V}(f) \\ u \geqq 1}} |u| = \text{card}\,(E_0^f) + s(f^0) + \text{card}\,(E_1^f) + s(f^1)$$

hence

$$|f| = s(f) - z(n) = |f^0| + |f^1| + er_f(\emptyset)\,.$$

Finally we prove the statement E. Let M be a model, card $(E) = n, f$ be a key for E. We prove it by induction on n:
1) Let $n = 2$. Then $|f| = 0$, $er_f(\emptyset) = 0$.
2) Suppose that E. holds for $k < n$. Let card $(E_0^f) > 1$, card $(E_1^f) > 1$.
Then by the Lemma

$$|f| = |f^0| + |f^1| + er_f(\emptyset) = \sum_{u \in \mathbf{D}(f^0)} er_{f^0}(u) + \sum_{u \in \mathbf{D}(f^1)} er_{f^1}(u) + er_f(\emptyset)\,.$$

Clearly for $v \in D(f^0)$ we have $er_{f^0}(v) = er(\text{card}\,((E_0^f)_{v*0}^{f^0}),\ \text{card}\,((E_0^f)_{v*1}^{f^0})) = = er(\text{card}\,(E_{0*v*0}^f), \text{card}\,(E_{0*v*1}^f)) = er_f(0 * v)$, similarly for f^1 and $\mathbf{D}(f^0) \cup \mathbf{D}(f^1) \cup \cup \{\emptyset\} = \mathbf{D}(f)$ and hence $|f| = \sum_{u \in \mathbf{D}(f)} er_f(u)$. For a key f such that card $(E_0^f) = 1$ or card $(E_1^f) = 1$ we proceed similarly.

In this Theorem we see at least a partial answer on our first question.

3.3. Corollary. Let $\mathscr{M}$ be a model, let f be a key for E on $\mathscr{M}$ and let g be a partial key for E. If $\sum_{u \in \mathbf{D}(g)} er_g(u) > s(f)$ then also $s(\bar{g}) = \sum_{u \in \mathbf{D}(\bar{g})} er_{\bar{g}}(u) \geqq s(f)$ for every key $\bar{g}$ which is an extension of g.

3.4. Theorem.

$$er(a, n - a) = 0 \equiv a \in I(n)$$

where

$$I(n) = \langle n - 2^{L_2(n)}, 2^{L_2(n)} \rangle \qquad \text{if} \quad n \geqq 3.2^{L_2(n)-1}$$

and

$$I(n) = \langle 2^{L_2(n)-1}, n - 2^{L_2(n)-1} \rangle \quad \text{if} \quad n \leqq 3.2^{L_2(n)-1}\,.$$

Proof. Let $n \geqq 3.2^{L_2(n)-1}$. We prove the statement in five steps:

1) $2^{L_2(n)-1} \leqq n - 2^{L_2(n)} < 2^{L_2(n)}$ and hence $L_2(n - 2^{L_2(n)}) = L_2(n) - 1$. Thus

$$er(n - 2^{L_2(n)}, 2^{L_2(n)}) = 2^{L_2(n)}(L_2(n) + 2) - 2^{L_2(n)+1} + \\ + (n - 2^{L_2(n)})(L_2(n) + 1) - 2^{L_2(n)} + n - n(L_2(n) + 2) + 2^{L_2(n)+1} = 0 .$$

2) $n - 2^{L_2(n)} \leqq a \leqq 2^{L_2(n)}$ iff $2^{L_2(n)} \geqq n - a \geqq n - 2^{L_2(n)}$.

3) Let $a \in I(n)$. By the symmetry of er we can suppose $a \geqq n - a$.

Assume $er(a, n - a) > 0$. Hence by Lemma in Theorem 3.2 $er(2^{L_2(n)}, n - 2^{L_2(n)}) > > 0$ which is a contradiction with 1)

4) $er(2^{L_2(n)} + 1, n - 2^{L_2(n)} - 1) = er(2^{L_2(n)}, n - 2^{L_2(n)}) + L_2(n) - (L_2(n) - 1) = = 1$.

5) Let $a \notin I(n)$. Then $er(a, n - a) > 0$ for if $a \geqq n - a$ then $a > 2^{L_2(n)}$ and hence $n - a < n - 2^{L_2(n)}$. Thus

$$er(a, n - a) \geqq er(2^{L_2(n)} + 1, n - 2^{L_2(n)} - 1) = 1 .$$

By the symmetry of er this holds also for $a < n - a$.

The proof of the case $n \leqq 3.2^{L_2(n)-1}$ is similar.

3.5. Remark. The interval $I(2^k)$ has only one element. The length of $I(n)$ increases with increasing distance of n from powers of 2, more exactly between numbers 2^k and 2^{k+1}, being greatest in $2^k + 2^{k-1}$. The length of the interval $I(2^k + 2^{k-1})$ is 2^{k-1}.

From Theorems 3.2 and 3.4 we have an answer to the second question:

3.6. Corollary. Let $\mathscr{M}$ be a model, f a key for E. Then $\bar{\mathbf{D}}(f)$ is an optimal tree iff $(\forall u \in \mathbf{D}(f))\,(er_f(u) = 0)$ i.e. iff $(\forall u \in \mathbf{D}(f))\,(\text{card}\,(E^f_{u*0}) \in I(\text{card}\,(E^f_u)))$.

4. ALGORITHMS

We now turn our attention to the key constructing algorithms. Let $\mathscr{M}$ be a model. Our attempt is to construct a key f for E on $\mathscr{M}$ which is optimal among all keys for E on $\mathscr{M}$ i.e. such that for every key g $s(g) \geqq s(f)$.

Published algorithms – as far as known to us [2], [3] – construct so called halving keys.

4.1. Definition. $\text{Sat}_A(k) = \{e \in A;\ \mathscr{M} \vdash k[e]\}$ where k is some elementary conjunction $\bigwedge_{i=1}^{m} \varepsilon_i \times P_i$.

4.2. Definition. A key f is *halving* if

$$(\forall u \in \mathbf{D}(f))\,(\forall_i = 1, \dots, k)\,(|\text{card}\,(E^f_{u*0}) - \text{card}\,(E^f_{u*1})| \leqq \\ \leqq |\text{card}\,(\text{Sat}_{E_u{}^f}\, P_i) - \text{card}\,(\text{Sat}_{E_u{}^f}\, \neg P_i)|).$$

Algorithms constructing halving key proceed in the obvious way: they start from the root and assign to each node that property which devides the respective set most symmetrically. We shall show that the halving key need not be optimal.

4.3. Theorem. There is a model $\mathscr{M}$ and two keys f and g for E such that f is halving key and g is not but g is better than f.

M:

	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8
P_1	0	0	0	0	1	1	1	1
P_2	0	0	0	1	1	1	1	1
P_3	0	0	0	1	1	0	0	0
P_4	1	0	0	0	0	1	0	0
P_5	0	1	0	0	0	0	1	0

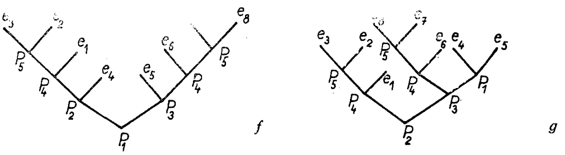


Fig. 1.

Proof. See fig. 1. The model $\mathscr{M} = \langle\{e_1, \ldots, e_8\}; \mathscr{P}_1, \ldots, \mathscr{P}_5\rangle$ is given by the matrix (by the definition of a model we use the corresponding functions $v_1, \ldots, v_5$). Two schemes represent functions f and g (the respective properties are added to nodes, respective objects to vertices and ordering on levels is lexicographic). Clearly f is a halving key and g is not, but

$$s(f) = 26 > 25 = s(g).$$

4.4. Definition. Let $\mathscr{M}$ be a model, f a partial key. We say that f is *complete on the level* j if

$$(\forall u \in \mathbf{D}(f))\,(|u| < j)\ \&\ (\forall u \in \mathbf{V}(f))\,(\text{card}\,(E_u^f) = 1 \vee |u| = j).$$

If f is a partial key we use $\bar{f}$ to denote an arbitrary extension of f.

We have shown that the halving key is not always optimal and that our optimal key need not be the halving one. This is true even if we consider the following modification of the definition of a halving key:

$$(\forall u \in \mathbf{D}(f))\,(\forall i = 1, \ldots, k)\,\big(er(\operatorname{card}(E^f_{u*0}), \operatorname{card}(E^f_{u*1})) \leqq \\ \leqq er(\operatorname{card}(\mathrm{Sat}_{E_u f}\, P_i), \operatorname{card}(\mathrm{Sat}_{E_u f}\, \neg P_i))\big)\,,$$

since otherwise we would obtain the following false statement as a corollary:

Let f, g be partial keys complete to the level 1 then

$$\Big(\sum_{\substack{u \in \mathbf{D}(f) \\ |u| < 1}} er_f(u) = er_f(\emptyset) < er_g(\emptyset) = \sum_{\substack{u \in \mathbf{D}(g) \\ |u| < 1}} er_g(u)\Big) \Rightarrow (\exists \bar{f})\,(\forall \bar{g})\,(s(\bar{f}) \leqq s(\bar{g}))\,.$$

Even a weaker statement is false:

Let $\mathscr{M}$ be a model (card $E = k$); f, g be partial keys complete to the level $l = L_2(k) - 2$ then

$$\Big[(\forall j \leqq L_2(k) - 2)\Big(\sum_{\substack{u \in \mathbf{D}(f) \\ |u| < j}} er_f(u) < \sum_{\substack{u \in \mathbf{D}(g) \\ |u| < j}} er_g(u)\Big)\Big] \Rightarrow (\exists \bar{f})\,(\forall \bar{g})\,(s(\bar{f}) \leqq s(\bar{g}))\,.$$

Instead, the contrary statement is true:

4.5. Theorem. For every l there is a model $\mathscr{M}$, a key g such that $\max_{u \in V(g)} |u| = l + 2$ and a partial key f such that $(\forall j \leqq l)\Big(\sum_{\substack{u \in \mathbf{D}(f) \\ |u| < j}} er_f(u) < \sum_{\substack{u \in \mathbf{D}(g) \\ |u| < j}} er_g(u)\Big)$ but nevertheless $(\forall \bar{f})\,(s(g) < s(\bar{f}))$.

Proof. First we prove the following

Lemma. Let $Z \in \mathscr{S}_n$ and let a number a_i assign to every $v_i \in \mathbf{V}(Z)$ $(i = 1, \ldots, n)$. Then there is a model $\mathscr{M}$, card $(E) = \sum_{i=1}^{n} a_i$ and a partial key f for E such that $\bar{\mathbf{D}}(f) = Z$ and card $(E^f_{v_i}) = a_i$ for $v_i \in \mathbf{V}(Z)$.

Proof. For $v_i \in \mathbf{V}(Z)$ we define $E_v = \{e^i_1, \ldots, e^i_{a_i}\}$ and we put $E = \bigcup_{v \in \mathbf{V}(Z)} E_v$. For the nodes we define $E_u = \{e \in E;\ e \in E_v\ \&\ v \in \mathbf{V}(Z)\ \&\ v \geqq u\}$. Then for every $u \in Z - \mathbf{V}(Z)$ we choose a property $\mathscr{P}^{(u)}$ such that $\mathscr{P}^{(u)}(e)$ iff $e \in E_{u*1}$. Let $\mathscr{P}_1, \ldots, \mathscr{P}_{u-1}$ be a sequence of all such defined properties. Then clearly $\mathscr{M} = \langle E, \mathscr{P}_1, \ldots, \mathscr{P}_{n-1}\rangle$ is a model and f defined by $f(u) = P_i$ if $\mathscr{P}_i = \mathscr{P}^{(u)}$ is a partial required key.

We now prove Theorem 4.5.

Let Z be a tree with $(2^{l+2} - 6)$ vertices: on the level l there are two vertices $u_1 = \langle 1, 0, \ldots, 0\rangle$ and $u_0 > 0$; other vertices are on the level $l + 2$. By the Lemma we construct a model $\mathscr{M}' = \langle E, P_1, \ldots, P_k\rangle$ and a partial key f such that card $(E^f_{u_0}) = 4$, card $(E^f_{u_1}) = 4$, card $(E^f_u) = 1$ if $u \in \mathbf{V}(Z)\ \&\ u \neq u_0\ \&\ u \neq u_1$. Clearly $er_f(u) = 0$ for $u \in \mathbf{D}(f)$. We choose $e_0 \in E^f_{u_0}$ and define a property $\mathscr{P}$: $\mathscr{P}(e)$ iff $e \in E^f_1 \cup \{e_0\}$.

On the model $\mathcal{M}'' = \langle E, \mathcal{P}_1, \ldots, \mathcal{P}_k, \mathcal{P}\rangle$ we define a partial key g: $g(\emptyset) = P$ and $g(u) = f(u)$ for $u \in \mathbf{D}(f)$ & $u \neq \emptyset$. From the construction of the model $\mathcal{M}'$ and definition of u_1 we see that $e_0 \in E^g_{u_1}$. We now have a similar situation as in Theorem 4.3:

$$\operatorname{card}\left(E^f_{u_0}\right) = 4\,, \quad \operatorname{card}\left(E^f_{u_1}\right) = 4\,, \quad \operatorname{card}\left(E^g_{u_0}\right) = 3\,, \quad \operatorname{card}\left(E^g_{u_1}\right) = 5\,.$$

Thus we can choose the properties $\mathcal{P}_{k+2}, \mathcal{P}_{k+3}, \mathcal{P}_{k+4}$ for $E^f_{u_0} \cup E^f_{u_1}$ corresponding to $\mathcal{P}_3, \mathcal{P}_4, \mathcal{P}_5$ of Theorem 4.3. On the model $\mathcal{M} = \langle E; \mathcal{P}_1, \ldots, \mathcal{P}_k, \mathcal{P}, \mathcal{P}_{k+2}, \ldots$ $\ldots, \mathcal{P}_{k+4}\rangle$ we define a key $\bar{g}$ as an extension of g such that $er_{\bar{g}}(u) = 0$ if $u \neq \emptyset$. Hence we have

$$(j \leqq l) \Rightarrow \sum_{\substack{u \in \mathbf{D}(f) \\ |u| < j}} er_f(u) = 0 < 1 = \sum_{\substack{u \in \mathbf{D}(\bar{g}) \\ |u| < j}} er_{\bar{g}}(u)$$

but for every extension $\bar{f}$ of f $er_{\bar{f}}(u_0) = 1$ & $er_{\bar{f}}(u_1) = 1$ thus $s(\bar{g}) < s(\bar{f})$. For illustration, we add schemes of the functions $\bar{f}$ and $\bar{g}$ for the case $l = 2$ (Fig. 2).

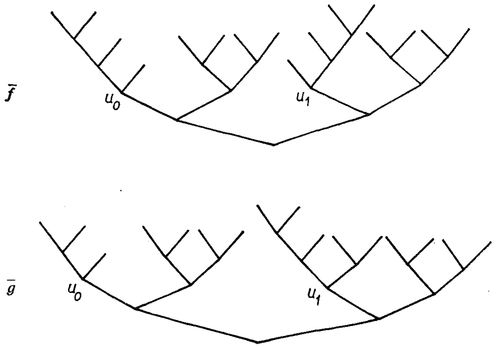


Fig. 2.

It is proposed in [3] to choose that property which allows good partition into two subsets for which there are good parting properties. Comparing partial keys with respect to their partial sums of errors is a more precise expression of this aim. But, we have seen that in order to get an optimal key (on $\mathcal{M}$) we must compare nearly the whole keys. In other words, before the construction of nearly the whole key is completed we cannot say if a key f with $f(\emptyset) = P$ is optimal.

So it seems that only two possibilities remain:

1) To construct nearly all keys and to compare them. In this case we can use the theory of error (Corollary 3.3) for eliminating bad keys: if we have some key f we

can eliminate every partial key having the sum of errors greater than the norm of f. However, without considerable improvements this method would obviously not be technically feasible at present. Its disadvantage comes also from practical aspects: if we need to modify an already existing key with respect to a larger number of objects. If we have an optimal key f for $A \subset E$ on $\mathscr{M}$ and if we look for an optimal key for E we must repeat the whole process of finding an optimal key for E because the key for E constructed as an extension of f need not be optimal for E.

2) Giving up the establishment of an optimal key the alternative is the construction of a key satisfactory in a certain sense, a locally optimal key (with respect to some metric, ordering or graph). Included here are procedures of correcting already available keys such as the method of transfer described in the sequel.

5. THE METHOD OF TRANSFER

At the end of the Section 4 we distinguished two possible kinds of procedures in constructing keys. In the frame of the second kind of procedures we propose a method of corrections of a given key. These corrections give a graph on the set of all keys on $\mathscr{M}$. We shall look for the locally best key (in the sense of criterion s) with respect to this graph.

The main principle is the following:

Let us have some key f for E on $\mathscr{M}$. By Theorem 4.3 it is possible to change in one node the corresponding property to another – maybe with a greater error – and to get in this way a better key. We shall define a key g originating from a given key f by a change of a property in one node and the different from f as little as possible.

5.1. Theorem. Let $(U, \leqq)$ be the canonical tree, V a non-empty subset of U such that

1) $(\forall u, v \in V)(u \wedge v \in V)$;

2) $(\forall u, v \in V)(u < v \Rightarrow (\exists z \in V)(u * \overline{\text{next}\,(u, v)} \leqq z))$ (where $\bar{0} = 1, \bar{1} = 0$).

Then there is a tree V' isomorphic to V.

Proof. Let $v \in V$. Then we can order the set $B_v = \{w; w \in V \,\&\, w \leqq v\}$ such that $B_v = \{w_1, \ldots, w_k\}$ and $w_1 < w_2 < \ldots < w_k = v$. Then we define a mapping ι as follows:

$$\iota(w_1) = \emptyset\,,$$

$$\iota(w_i) = \iota(w_{i-1}) * \text{next}\,(w_{i-1}, w_i)\,,$$

$$\iota(v) = \iota(w_{k-1}) * \text{next}\,(w_{k-1}, v)\,.$$

ι is one-one and preserves the ordering: if $w, z \in V$ then either $w < z$ and then $\iota(w) < \iota(z)$ or $w \parallel z$ and then $w \wedge z \in V$ and $\text{next}\,(w \wedge z, w) \neq \text{next}\,(w \wedge z, z)$ hence $\iota(w) \neq \iota(z)$.

We now show that $V' = \iota'' V$ is a tree: V' is non-empty and finite subset of U.

By the definition of ι, $\iota''\{w; w \in V \,\&\, w \leqq v\} = \{u; u \leqq \iota(v)\} \subseteqq V'$.

Let $u \in V'$, $u * \varepsilon \in V'$ where $\varepsilon \in \{0, 1\}$. Let $z = \min_{\leqq} \{v; v \in V \,\&\, v \geqq \iota^{-1}(u) * \bar{\varepsilon}\}$. Clearly $\operatorname{next}(v, w) = \operatorname{next}(\iota(v), \iota(w))$ for $v, w \in V$ and hence $\iota(z) = \iota(\iota^{-1}(u)) * * \operatorname{next}(\iota(\iota^{-1}(u)), z) = u * \bar{\varepsilon}$.

Thus $u * \bar{\varepsilon} \in V'$.

This completes the proof.

Remark. The mapping ι will be very useful for our further consideration.

In sequel, let $\mathscr{M}$ be a fixed model. Hence saying f is a key for E we mean a key for E on $\mathscr{M}$.

Let f be a key for E. We want to define a key for $A \subseteq E$ induced by f.

5.2. Definition. Let f be a key for E, $\emptyset \neq A \subseteq E$.

$\operatorname{Reg}(A, f) = \{u \in \bar{\mathbf{D}}(f); (E^f_{u*1} \cap A \neq \emptyset \,\&\, E^f_{u*0} \cap A \neq \emptyset) \vee (u \in \mathbf{V}(f) \,\&\, E^f_u \in A)\}$ is the *set of regular elements* of $\bar{\mathbf{D}}(f)$ with respect to f and A. $\operatorname{Sing}(A, f) = \bar{\mathbf{D}}(f) \setminus \setminus \operatorname{Reg}(A, f)$ is the *set of singular elements* of U.

5.3. Theorem. The set $\operatorname{Reg}(A, f)$ is isomorphic to a tree.

Proof. We show that $\operatorname{Reg}(A, f)$ satisfies the assumptions from Theorem 5.1: $A \neq \emptyset$ implies $\operatorname{Reg}(A, f) \neq \emptyset$. $\operatorname{Reg}(A, f) \subseteqq \bar{\mathbf{D}}(f)$ hence it is finite. Assume $u, v \in \in \operatorname{Reg}(A, f)$. Then clearly $E^f_u \cap A \neq \emptyset$ and $E^f_v \cap A \neq \emptyset$. If $u \leqq v$ then $u \wedge v = = u \in \operatorname{Reg}(A, f)$. Similarly for $v < u$. If $u \parallel v$ and $u \neq v$ then $E^f_{(u \wedge v)*\operatorname{next}(u \wedge v, u)} \cap \cap A \geqq E^f_u \cap A \neq \emptyset$ and also $E^f_{(u \wedge v)*\operatorname{next}(u \wedge v, v)} \cap A \neq \emptyset$ hence $u \wedge v \in \operatorname{Reg}(A, f)$. Let $u, v \in \operatorname{Reg}(A, f)$, $u < v$. Then $E^f_{u*\overline{\operatorname{next}(u,v)}} \cap A = A' \neq \emptyset$ and hence there is a vertex $w \geqq u * \overline{\operatorname{next}(u, v)}$ such that $E^f_w \subseteqq A'$.

Thus $w \in \operatorname{Reg}(A, f)$.

By Theorem 5.1 there is an isomorphism ι of the set $\operatorname{Reg}(A, f)$ onto a tree $\iota'' \operatorname{Reg}(A, f)$.

5.4. Definition. We define a function $f \downarrow A$ for $A \subseteqq E$ and f a key for E by letting

$$\mathbf{D}(f \downarrow A) = \{u \in \iota'' \operatorname{Reg}(A, f); u * 0 \in \iota'' \operatorname{Reg}(A, f)\} ;$$

$$(f \downarrow A)(u) = f(\iota^{-1}(u)) \quad \text{for} \quad u \in \mathbf{D}(f \downarrow A) .$$

5.5. Theorem. $(f \downarrow A)$ is a key for A.

Proof. First we show $A^u_{f \downarrow A} = A \cap E^f_{\iota^{-1}(u)}$. Clearly, it suffices to prove $\mathscr{M} \vdash k(u)\,[e]$ iff $\mathscr{M} \vdash k^R(u)\,[e]$ for $u \in \operatorname{Reg}(A, f)$ and for $e \in A$ where

$$k^R(u) = \bigwedge_{\substack{w < u \\ w \in \operatorname{Reg}(A, f)}} \operatorname{next}(w, u) \times f(w) .$$

Obviously if $\mathcal{M} \vdash k(u)\,[e]$ then $\mathcal{M} \vdash k^R(u)\,[e]$. Let $\mathcal{M} \vdash k^R(u)\,[e_1]$ and $\mathcal{M} \vdash \neg k(u)\,.\,[e_1]$ for some $e_1 \in A$. Since $u \in \operatorname{Reg}(A, f)$ we have $\mathcal{M} \vdash k^R(u)\,[e_2]$ and $\mathcal{M} \vdash k(u)\,[e_2]$ for some $e_2 \in A$. This implies the existence of a $v \in \operatorname{Sing}(A, f)$ such that $v < u$ and

$$\mathcal{M} \vdash \overline{\text{next}\,(v, u)} \times f(v)\,[e_1]\,,$$

$$\mathcal{M} \vdash \text{next}\,(v, u) \times f(v)\,[e_2]$$

which is a contradiction.

We can now prove that $f \downarrow A$ is a key for A.
In fact

1) for $u \in \overline{\mathbf{D}}(f \downarrow A)$ we have $A^u_{f\downarrow A} = E^f_{\iota^{-1}(u)} \cap A$ which is non-empty because $\iota^{-1}(u) \in \operatorname{Reg}(A, f)$;
2) $(\forall e \in A)\,(\exists v \in \mathbf{V}(f))\,(E^f_v = \{e\})$ hence $\iota(v) \in \overline{\mathbf{D}}(f \downarrow A)$ and $A^{f\downarrow A}_{\iota(v)} = \{e\}$.

Remark. For card $(A) = 1$ we have $\mathbf{D}(f \downarrow A) = \emptyset$ and $\overline{\mathbf{D}}(f \downarrow A) = \{\emptyset\}$.

Denotation. Let $a \neq e$ are two elements of E. We denote by P_{ae} the first predicate symbol P for which $\mathcal{M} \vdash P[a]$ iff $\mathcal{M} \vdash \neg P[e]$ (in the ordering of indices). (By the assumption on $\mathcal{M}$ there is always such a predicate symbol.)

5.6. Definition. Let f be a key for $A \subset E$, $e \in E \setminus A$. We define a function f_e as follows: $\mathbf{D}(f_e) = \mathbf{D}(f) \cup \{u\}$ where u is the vertex such that $\mathcal{M} \vdash k(u)\,[e]$. (By Lemma 2.5 there is exactly one such vertex.) For $v \in \mathbf{D}(f)$ let $f_e(v) = f(v)$ and $f_e(u) = P_{ae}$ where $E^f_u = \{a\}$.

5.7. Lemma. f_e is a key for $A \cup \{e\}$.
Proof. Obvious.

5.8. Definition. Let $(U, \leqq)$ be the canonical tree, f a tree-function to the set of predicate symbols, $v \in U$. We define a function $sh(f, v)$ (shift) as follows:

$$\mathbf{D}(sh(f, v)) = \{u;\, u = v * q \;\&\; q \in \mathbf{D}(f)\}\;;$$

$$sh(f, v)\,(u) = f(q) \quad \text{for} \quad u \in \mathbf{D}(sh(f, v)) \quad \text{i.e.} \quad u = v * q\,.$$

5.9. Lemma. Let f be a partial key for E, let g^u be partial keys for the sets E^f_u if card $(E^f_u) \geqq 2$ & $u \in \mathbf{V}(f)$. Then the function $\bar{f} = f \cup \bigcup_{\substack{u \in \mathbf{V}(f) \\ \text{card}(E_u{}^f) \geqq 2}} sh(g^u, u)$ is a key for E.

Proof. We put $\mathbf{V}'(f) = \{u \in \mathbf{V}(f);\, \text{card}\,(E^f_u) \geqq 2\}$ then

$$\mathbf{D}(\bar{f}) = \mathbf{D}(f) \cup \bigcup_{u \in \mathbf{V}'(f)} \{u * q;\; q \in \mathbf{D}(g^u)\}\;;$$

$$\overline{\mathbf{D}}(\bar{f}) = \overline{\mathbf{D}}(f) \cup \bigcup_{u \in \mathbf{V}'(f)} \{u * q;\; q \in \overline{\mathbf{D}}(g^u)\}\,.$$

We show that $\bar{f}$ is a key for E: Assume $u \in \bar{\mathbf{D}}(\bar{f})$. Then either $u \in \mathbf{D}(f)$ and $E_u^{\bar{f}} = E_u^f \neq \emptyset$ or $u = v * q$ & $q \in \bar{\mathbf{D}}(g^v)$ and $E_u^{\bar{f}} = (E_v^f)_q^{g^v} \neq \emptyset$.

Let $e \in E$. By Lemma 2.5 there is just one vertex $u \in \mathbf{V}(f)$ such that $e \in E_u^f$. Either $\operatorname{card}(E_u^f) = 1$ or $\operatorname{card}(E_u^f) \geqq 2$. But then there is a key g^u for E_u^f; $q \in \mathbf{V}(g^u)$ and for $v = u * q \in \bar{\mathbf{D}}(\bar{f})$ we have $E_v^{\bar{f}} = (E_u^f)_q^{g^u} = \{e\}$.

5.10. Definition. Let f be a key for E. We say that f *is transferable through the node $u \in \mathbf{D}(f)$ with the help of property $\mathscr{P}$* if there are $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$ for which

$$E_{u*\varepsilon_1}^f \subsetneqq \operatorname{Sat}_{E_u f}(\varepsilon_2 \times P) \subsetneqq E_u^f .$$

Denotation. Let $k = \bigwedge_{i=1}^{n} \varepsilon_i \times P_i$ be an elementary conjunction. The formulas $\varepsilon_i \times P_i$ are called literals. We denote by $k[P/Q]$ the conjunction resulting from k by substituting a literal Q for a literal P.

5.11. Definition. Let f be a key for E, let f be transferable through $u \in \mathbf{D}(f)$ with the help of P. We define the function g *resulting from f by the transfer through the node u with the help of P* (we write $g = \operatorname{Trf}(f, u, P)$) as follows:

I. Let

$$E_{u*\varepsilon}^f \subset \operatorname{Sat}_{E_u f}(\varepsilon \times P) \subset E_u^f .$$

We call $A = \operatorname{Sat}_{E_u f}(\varepsilon \times P) - E_{u*\varepsilon}^f$ the transferred set.

1) $g'(v) = f(v)$ if $v \in \mathbf{D}(f)$ & $(v < u \vee v \parallel u \vee v \geqq u * \varepsilon)$;

2) $g'(u) = P$;

3) $g^{u*\bar{\varepsilon}} = f \downarrow (E_{u*\bar{\varepsilon}}^f \setminus A)$;

4) let $w_j > u * \varepsilon$ be a vertex $(E_{w_j}^f = \{e_j\})$ such that $\operatorname{Sat}_{E_u f}(k(w_j)[\varepsilon \times f(u)/\varepsilon \times P] - \{e_j\} = A_j \neq \emptyset$ then $g^{w_j} = (f \downarrow A_j)_{e_j}$. Finally $g = g' \cup sh(g^{u*\bar{\varepsilon}}, u * \bar{\varepsilon}) \cup \bigcup_{w_j} (g^{w_j}, w_j)$.

II. Let $E_{u*\bar{\varepsilon}}^f \subset \operatorname{Sat}_{E_u f}(\varepsilon \times P) \subset E_u^f$. In this case we call $A = \operatorname{Sat}_{E_u f}(\varepsilon \times P) \setminus E_{u*\bar{\varepsilon}}^f$ the transferred set. (In both cases we transfer the set A from one subset of E_u^f to another.)

1) $g'(v) = f(v)$ if $v \in \mathbf{D}(f)$ & $(v < u \vee v \parallel u)$;

2) $g'(u) = P$;

3) $g^{u*\bar{\varepsilon}} = f \downarrow (E_{u*\varepsilon}^f \setminus A)$;

4) let $w_j \geqq u * \bar{\varepsilon}$ be a vertex $(E_{w_j}^f = \{e_j\})$ such that $\operatorname{Sat}_{E_u f}(k(w_j)[\bar{\varepsilon} \times f(u)/\varepsilon \times P]) - \{e_j\} = A_j \neq \emptyset$. Then $g^{w_j} = (f \downarrow A_j)\, l_j$ and $g^{u*\varepsilon} = f^{u*\bar{\varepsilon}} \cup \bigcup_{w_j} sh(g^{w_j}, w_j)$.

Finally $g = g' \cup sh(g^{u*\bar{\varepsilon}}, u * \bar{\varepsilon}) \cup sh(g^{u*\bar{\varepsilon}}, u * \bar{\varepsilon})$.

5.12. Lemma. g is a key for E.

Proof. I. g' is a partial key. $\mathbf{V}(g')$ consists of

1) $u * \bar{\varepsilon}$ and then $E_{u*\bar{\varepsilon}}^{g'} = E_{u*\bar{\varepsilon}}^f \setminus A \neq \emptyset$;

2) $w_j \geqq u * \varepsilon$ and then $E^{g'}_{w_j} = \mathrm{Sat}_{E_u{}^f}(k(w_j)\,[\varepsilon \times f(u)/\varepsilon \times P])$;
3) v and then $\mathrm{card}\,(E^{g'}_v) = 1$.
Hence by Theorem 5.5 and by Lemma 5.9 g is a key for E.

II. First we show that $g^{u*\varepsilon}$ is a key for $E^{g'}_{u*\varepsilon} = E^f_{u*\bar{\varepsilon}} \cup A$. $f^{u*\bar{\varepsilon}}$ is a partial key for $E^{g'}_{u*\varepsilon}$ and $\mathbf{V}(f^{u*\bar{\varepsilon}})$ consists of:
1) w_j and then $E^{f^{u*\bar{\varepsilon}}}_{w_j} = \mathrm{Sat}_{E^f_{u*\bar{\varepsilon}} \cup A}(k(w_j)) = A_j \cup \{e_j\}$;
2) v and then $\mathrm{card}\,(E^{f^{u*\bar{\varepsilon}}}_v) = 1$.
Hence by Theorem 5.5 and by Lemma 5.9 $g^{u*\varepsilon}$ is a key for $E^{g'}_{u*\varepsilon}$.
Similarly as in part I. we can prove that g is a key for E.

We shall now consider all keys for E with respect to the passing from one key to another by transfer.

5.13. Definition. Let $G_{\mathscr{M}} = \{f; f \text{ is a key for } E \text{ on } \mathscr{M}\}$,

$$R = \{\langle f, g\rangle; f, g \in G_{\mathscr{M}} \;\&\; (\exists u \in D(f))\,(\exists P)\,(g = \mathrm{Trf}\,(f, u, P))\}\,.$$

Then $\langle G_{\mathscr{M}}, P\rangle$ is called the *oriented graph of transfers.*

5.14. Lemma. If $\langle f, g\rangle \in R$ then there are uniquely determined u and P such that $g = \mathrm{Trf}\,(f, u, P)$.

Proof. $u = \min_{\leqq} \{v; f(v) \neq g(v)\}$ obviously such minimum is only one; then $P = g(u)$.

Remark. If $g = \mathrm{Trf}\,(f, u, P)$ then $h = \mathrm{Trf}\,(g, u, f(u))$ is also a key.

5.15. Lemma. The graph $\langle G_{\mathscr{M}}, R\rangle$ is not generally symmetric, i.e. it is not true that for every model $\mathscr{M}$ and for arbitrary keys f, g for E we have $\langle f, g\rangle \in R \Rightarrow \langle g, f\rangle \in R$.

Proof. We shall describe a model $\mathscr{M} = \langle\{e_1, \ldots, e_4\}, \mathscr{P}_1, \ldots, \mathscr{P}_4\rangle$ and two keys f and g for E such that $g = \mathrm{Trf}\,(f, \emptyset, P_2)$, i.e. $\langle f, g\rangle \in R$. Nevertheless $\langle g, f\rangle \notin R$ because $h = \mathrm{Trf}\,(g, \emptyset, f(u)) \neq f$ and there is no other transfer which can change $g(\emptyset)$ to $f(\emptyset)$. The model $\mathscr{M}$ is given by the matrix, keys f, g, h by their schemes; to each node we add assigned property, to each vertex the corresponding object (Fig. 3).

5.16. Definition. A key $g \in G_{\mathscr{M}}$ is *accessible* from f in $\langle G_{\mathscr{M}}, R\rangle$ if there is a sequence $h_1, \ldots, h_n$ of elements of $G_{\mathscr{M}}$ such that $f = h_1 \;\&\; g = h_n \;\&\; (\forall i = 1, \ldots, n-1)\,(\langle h_i, h_{i+1}\rangle \in R)$.

5.17. Lemma. There are keys f, g such that g is not accessible from f.

Proof. There is a simple model $\mathscr{M}$ where there are only two keys f and g and no transfer exists. Thus g is not accessible from f and more f is not accessible from g.

5.18. Definition. For every $f \in G_{\mathscr{M}}$ we define a set R_f of all keys $g \in G_{\mathscr{M}}$ accessible from f in $\langle G_{\mathscr{M}}, R\rangle$.

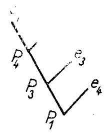
Remark. For every $f \in G_{\mathcal{M}}$ R_f is not empty and by Lemma 5.17 it can be a proper subset of $G_{\mathcal{M}}$.

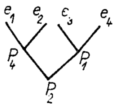
5.19. Definition. Let $S = \{\langle f, g\rangle;\ f, g \in G_{\mathcal{M}}\ \&\ \langle f, g\rangle \in R\ \&\ s(g) < s(f)\}$ then $\langle G_{\mathcal{M}}, S\rangle$ is called the *oriented graph of improving transfers.*

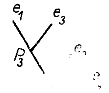
M:

	e_1	e_2	e_3	e_4
P_1	0	0	0	1
P_2	0	0	1	1
P_3	0	0	1	0
P_4	0	1	0	0

f







$g = \mathrm{Trf}\,(f, \emptyset, P_2)$ $h = \mathrm{Trf}\,(g, \emptyset, f(\emptyset))$

Fig. 3.

5.20. Definition. Similarly as in Definition 5.16 we define a set S_f of all keys $g \in G_{\mathcal{M}}$ accessible from f in $\langle G_{\mathcal{M}}, S\rangle$.

5.21. Definition. We say that f is a *local minimum* in the graph $\langle G_{\mathcal{M}}, S\rangle$ if there is no $g \in G_{\mathcal{M}}$ such that $\langle f, g\rangle \in S$.

Let f be a key for E. We shall try to find some local minimum accessible from f. By Lemma 5.17 we see that the best key for E need not be accessible from f. Since not even all keys accessible from f can be constructed we shall find some local minimum in an estimate number of steps.

We now deduce some Lemmas for the algorithm proposed later.

5.22. Definition. Let f be a key for E, $g = \mathrm{Trf}\,(f, u, P)$. We define a function F from $\mathsf{D}(f)$ $(\mathsf{D}(F) \subseteq \mathsf{D}(f))$ to $\mathsf{D}(g)$ as follows:

In the case I. from Definition 5.11, when $E^f_{u*\varepsilon} \subset \varepsilon \times P \subset E^f_u$ and $A = \mathrm{Sat}_{E_u f}(\varepsilon \times \times P) - E^f_{u*\varepsilon}$ is the transferred set we put

$$F(v) = v \text{ for } v \in \mathsf{D}(f)\ \&\ (v \leqq u \vee v \parallel u \vee v \geqq u * \varepsilon)$$

and

$$F(v) = u * \bar{\varepsilon} * \iota(v) \text{ for } v \in \mathbf{D}(f) \mathbin{\&} v \geqq u * \bar{\varepsilon},$$

where ι is a mapping from the definition of the function $f \downarrow (E^f_{u*\bar{\varepsilon}} \setminus A)$.

In the case II., when $E^f_{u*\varepsilon} \subset \bar{\varepsilon} \times P \subset E^f_u$ and $A = \mathrm{Sat}_{E_u f}(\bar{\varepsilon} \times P) - E^f_{u*\varepsilon}$ is the transferred set we put

$$F(v) = v \text{ for } v \in \mathbf{D}(f) \mathbin{\&} (v \leqq u \vee v \parallel u)$$

and

$$F(v) = l_u(v) \text{ for } v \in \mathbf{D}(f) \mathbin{\&} v \geqq u * \bar{\varepsilon}$$

and

$$F(v) = l_u(u * \varepsilon * \iota(v)) \text{ for } v \in \mathbf{D}(f) \mathbin{\&} v \geqq u * \varepsilon$$

where ι is the mapping from the definition of the function $f \downarrow (E^f_{u*\varepsilon} \setminus A)$ and l_u maps the set $\{v; v \geqq u\}$ onto itself as follows: $l_u(v) = l_u(u * \varepsilon * q) = u * \bar{\varepsilon} * q$.

5.23. Lemma. Let f be a key for E, $A \subset E$ and let $E^f_u \subseteq A$. Then $(f \downarrow A)^{\iota(u)} = f^u$.

Proof. By the definition of ι, if $\{v; u \leqq v \leqq w\} \subseteq \mathrm{Reg}(f, A)$ then $w = u * q \Rightarrow \Rightarrow \iota(w) = \iota(u) * q$. By Theorem 5.5 $E^{f \downarrow A}_{\iota(u)} = E^f_u \cap A = E^f_u$ hence f^u and $(f \downarrow A)^{\iota(u)}$ are keys for E^f_u. If $q \in \mathbf{D}(f^u)$ then $f^u(q) = f(u * q) = (f \downarrow A)(\iota(u * q)) = (f \downarrow A) . . (\iota(u) * q) = (f \downarrow A)^{\iota(u)}(q)$.

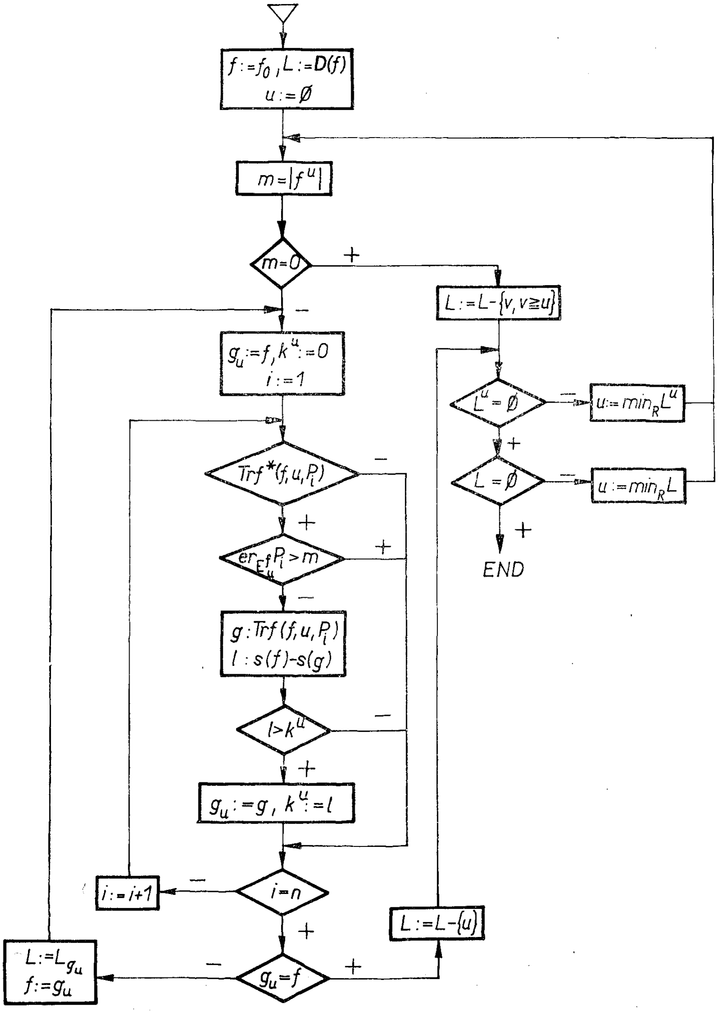
5.24. Lemma. Let f be a key for $A \subseteq E$, g a key for E and $\mathbf{D}(f) \subseteqq \mathbf{D}(g) \mathbin{\&} (\forall v \in \in \mathbf{D}(f))(f(v) = g(v))$. Then $f = g \equiv A = E$.

Proof. Obvious.

5.25. Definition. Let f be a key for E, $g = \mathrm{Trf}(f, u, P)$, A be the transferred set. Then we define a set L^{fg}_u (*a set of "suspicious nodes" after transfering in* u) as follows: $L^{fg}_u = \{w \in \mathbf{D}(g); E^f_{F^{-1}(w)} \cap A \neq \emptyset\} \cup \{v \in \mathbf{D}(g); E^g_v \cap A \neq \emptyset\}$.

Fig. 4. Flow diagram — INPUT $\mathscr{M} = \langle E, \mathscr{P}_1, \ldots, \mathscr{P}_k \rangle, f_0$

1. Linear ordering R is the extension of partial ordering of canonical tree, which is lexicographic on levels;
2. $s(f) = \sum_{v \in \mathbf{V}(f)} |v|$;
3. $\mathbf{D}(f^u) = \{q; u * q \in D(f)\}, f^u(q) = f(u * q)$, viz 3.2;
4. $|f^u| = s(f^u) - z(\mathrm{card}\,(E^f_u))$, viz 3.2;
5. Trf* (f, u, P_i) iff f is transferable through the node u with the help of P_i, viz 5.10;
6. $g = \mathrm{Trf}\,(f, u, P)$ viz 5.11;
7. L_f set of "suspicious nodes" with respect to f, viz 5.27;
8. $L^u = \{v \in L; v \geqq_R u\}$.


$f:=f_0, L:=D(f)$
$u:=\emptyset$
$m=|f^u|$
$m=0$
+
−
$L:=L-\{v, v\geqq u\}$
$g_u:=f, k^u:=0$
$i:=1$
$L^u=\emptyset$
−
$u:=\min_R L^u$
+
$L=\emptyset$
−
$u:=\min_R L$
+
END
$Trf^*(f,u,P_i)$
−
+
$er_{E_u}fP_i>m$
+
−
$g:Trf(f,u,P_i)$
$l:s(f)-s(g)$
$l>k^u$
−
+
$g_u:=g, k^u:=l$
$i:=i+1$
−
$i=n$
+
$L:=L-\{u\}$
$L:=L_{g_u}$
$f:=g_u$
−
$g_u=f$
+

5.26. Lemma. Let f be a key for E, $g = \mathrm{Trf}\,(f, u, P)$. Then $v \in \mathbf{D}(g)\ \&\ v \notin L_u^{fg} \Rightarrow$ $\Rightarrow (\exists w)\,(w \in \mathbf{D}(f)\ \&\ g^v = f^w)$.

Proof. If $v \parallel u$ then obviously $f^v = g^v$. If $v > u\ \&\ v \notin \mathbf{W}(F)$ then (by the definition of g and F) $E_v^g \cap A \neq \emptyset$; hence $v \in L_u^{fg}$.

Let $v > u\ \&\ v \in \mathbf{W}(F)$. Then in the case I. from Definitions 5.11 and 5.22 we have the following:

1) If $F(v) = v$ then $v \geqq u * \varepsilon$ hence $E_v^f \subseteqq E_{u*\varepsilon}^f\ \&\ E_{u*\varepsilon}^f \cap A = \emptyset$. Thus we must show: $E_w^g \cap A = \emptyset \equiv g^w = f^w$. By the definition of g,

$$(\forall w \geqq v)\,(w \in \mathbf{D}(f^v) \Rightarrow w \in \mathbf{D}(g^v)\ \&\ g^v(w) = f^v(w)\ \&\ E_v^f \subseteqq E_v^g)\,.$$

By Lemma 5.24, $f^v = g^v \equiv E_v^g = E_v^f \equiv E_v^g \cap A = \emptyset$.

2) If $F(v) = w$ where $v = u * \bar{\varepsilon} * g\ \&\ w = u * \bar{\varepsilon} * \iota(v)$ then $E_w^g \subseteqq E_{u*\bar{\varepsilon}}^g\ \&\ E_{u*\bar{\varepsilon}}^g \cap$ $\cap A = \emptyset$. Hence we must show: $E_v^f \cap A = \emptyset \equiv f^v = g^w$. By the definition of g, $g^w = (f \downarrow (E_{u*\bar{\varepsilon}}^f \setminus A))^{\iota(v)} = f^v \equiv E_{u*\varepsilon}^f \setminus A \supseteqq E_v^f \equiv E_v^f \subseteq E_{u*\varepsilon}^f\ \&\ E_v^f \cap A = \emptyset \equiv E_v^f \cap$ $\cap A = \emptyset$.

In the case II. we proceed similarly.

5.27. Denotation. Let L_f be a set of "suspicious nodes" with respect to f then

$$\begin{aligned} L_g = F''(L_f) \cup L_u^{fg} = (L_f \cap \{v;\ v \parallel u\}) \cup \{v;\ v \geqq u\} \cup \\ \cup \{F(v) \geqq u * \bar{\varepsilon};\ v \in \mathbf{D}(f)\ \&\ (E_v^f \cap A \neq \emptyset \vee v \in L_f)\} \cup \\ \cup \{v \geqq u * \varepsilon;\ v \in \mathbf{D}(g)\ \&\ (E_v^g \cap A \neq \emptyset \vee v \in L_f)\}\,. \end{aligned}$$

We shall now present a flow-diagram (Fig. 4) of an algorithm for searching a local minimum accessible from a given key f.

From the above Lemmas we see that the algorithm searches the local minimum in the following way: It goes through the set L of "suspicious nodes" (which at the beginning equals to the whole $\mathbf{D}(f)$) and tries to construct in the node u the best improving transfer. If such transfer is found the algorithm tries again on the new key to construct the best transfer in the node u. If no improving transfer exists it proceeds to another element of L and u is no more a suspicious node. Through every transfer new suspicious nodes might be added. By Lemma 5.26 in other nodes not belonging to L an improving transfer cannot exist. The process ends as soon as the set L is empty, i.e. as soon as in no node an improving transfer can be constructed. If during some tree-traversing the key f is not modified then $L = \emptyset$. Thus we can estimate the length of the process: Consider the worst situation characterized by the following conditions

a) at the end we get the best key with norm equal zero;

b) during every tree-traversing maximally one transfer improving about one is constructed and at the same time L extends to $\mathbf{D}(f)$;

c) in every node u we can use every property (being obviously never the case).

Then during the whole process $m.k.(n - 1)$ transfers must be tested where m is the norm of original key f_0, $n - 1$ is a number of nodes in $\mathbf{D}(f)$ and k is a number of properties. Thus the number of tested transfers in every process must be less than $m.(n - 1).k$.

(Received May 8, 1973.)

REFERENCES

[1] Joseph R. Shoenfield: Mathematical Logic. Addison-Wesley Publ. Comp., Reading, Massachusetts—Menlo Park, California—London—Don Mills, Ontario 1967.

[2] R. Jičín, Z. Pilous, Z. Vašíček: Grundlagen einer formalen Methode zur Zusammenstellung und Bewertung von Bestimmungsschlüsseln. Preslia 41 (1969), p. 71—85.

[3] R. Hall: A Computer-based System for Forming Identification Keys. Taxon 19 (1970), 1.

[4] D. V. Osborne: New Aspects of the Theory of Dichotomous Keys. New Phytologist (1962).

Dr. Kamila Bendová, Matematický ústav ČSAV (Mathematical Institute — Czechoslovak Academy of Sciences), Žitná 25, 115 67 Praha 1. Czechoslovakia.