Journal of the Operations Research
Society of Japan
Vol. 23, No. 4, December 1980

A GRAPHICAL APPROACH TO THE PROBLEM OF LOCATING THE ORIGIN OF THE SYSTEM FAILURE

Masao Iri, *University of Tokyo,*
Eiji O'Shima, *Tokyo Institute of Technology,*
and
Katsuaki Aoki, *Mitsubishi Heavy Industries*
Hisayoshi Matsuyama, *Kyushu University*

(Received June 21, 1978; Final January 12, 1980)

Abstract This paper presents a way of formulating the problem of locating the origin of a system failure. A signed digraph is used for a mathematical model representing the influences among elements of the system, and the concept of a pattern on the signed digraph is introduced for representing a state of the system. The representations are quite rough and qualitative. The origin of a failure of the system can be located in terms of these concepts. It is further pointed out that, even when the pattern can be observed partially, the assumption of a single origin of the failure enables us to restrict the possible range of the origin to some extent.

1. Graphical Representation of a System and Its State

In recent years, graphical representations have been proved to be useful for modelling and analyzing various kinds of systems in many fields of science and engineering.

When a directed graph (or, for short, a digraph) is used as a mathematical model of a system, its nodes represent the elements of the system and its branches represent the immediate influences among the elements. In order to distinguish between positive and negative influences (for instance, between reinforcement and suppression), a signed digraph is defined formally as follows. As for the terminology and notation about graphs, we shall largely follow [1].

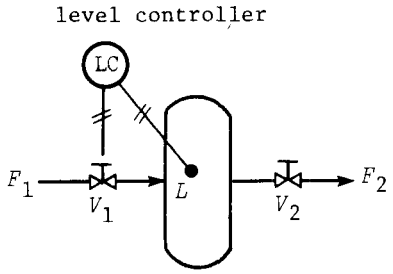
Definition 1. A *signed digraph* S is the composite concept (G, ψ) of
(i) a digraph G which is the quadruple $(N, B, \partial^+, \partial^-)$ of
(a) a set of nodes $N = \{\mathbf{n}_1, \mathbf{n}_2, \cdots, \mathbf{n}_M\}$,
(b) a set of branches $B = \{\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n\}$,

(c) a couple of incidence relations $\partial^+ : B \to N$ and $\partial^- : B \to N$ which make each branch correspond to its initial node and its terminal node, respectively,

and

(ii) a function $\psi : B \to \{+, -\}$, where $\psi(\mathbf{b}_k)$ $(\mathbf{b}_k \in B)$ is called the *sign of branch* $\mathbf{b}_k$. ☒

Example 1. An illustrative example of a signed digraph: --- Let a branch with sign +(-) indicate the relation such that, if the value of the state variable represented by the initial node of the branch is greater than the normal value, the value of the state variable represented by the terminal node becomes greater (smaller) than the normal value. Then, the influences among the state variables of the water tank system of Fig. 1 are represented by the signed digraph of Fig. 2. ☒



F_1, F_2: Flows

V_1, V_2: Apertures of valves

L: Level of the water in the tank

Fig. 1. Simple water tank system as an illustrative example

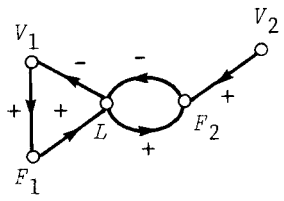


Fig. 2. Signed digraph for the water tank system of Fig. 1

We shall assume that the state of the system is specified by whether the quantity associated with each element (to be called the state variable of the element) takes the "normal" value, is greater or smaller than it. The three states of the quantity are designated, respectively, as "0", "+" and "-". Thus, the state of the system is described by assigning any of the three symbols 0, + and - to each node of the signed digraph representing the structure of the system. Formally, the states may be defined in terms of "patterns" as follows.

Definition 2. A *pattern* on the signed digraph $S = (G, \psi)$ is a function $\omega : N \to \{+, 0, -\}$. $\omega(\mathbf{n}_\alpha)$ $(\mathbf{n}_\alpha \in N)$ is called the *sign of node* $\mathbf{n}_\alpha$. ☒

Example 2. In the water tank system of Fig. 1, a state of the system can be described by assigning the sign 0, +, or - to each node according as the value of the variable corresponding to the node lies within, above or below the prescribed interval of tolerance, respectively. If any node has a sign + or -, the system is in failure. ☒

For a given signed digraph and an observed pattern on it, it is natural to consider that the manner of propagation of the failure is represented by the *cause-effect graph* (or, for short, the *CE graph*) defined as follows.

Definition 3. Given a pattern ω on a signed digraph $S = (G, \psi)$, a branch $\mathbf{b}_K$ is said to be *consistent* (with ω) if $\omega(\partial^+\mathbf{b}_K)\psi(\mathbf{b}_K)\omega(\partial^-\mathbf{b}_K) = +$, and a node $\mathbf{n}_\alpha$ is said to be *valid* if $\omega(\mathbf{n}_\alpha) \neq 0$, where the operations on signs are defined as usual, i.e., we assume $(+) \times (+) = (-) \times (-) = +$ and $(+) \times (-) = (-) \times (+) = -$. The subgraph G^* of G which consists of all the valid nodes and all the consistent branches is called the *CE graph* for the pattern ω on the signed digraph S. ☒

When the CE graph is decomposed into strongly connected components with the partial order among them [1], the system failure is reasonably thought to originate from among the elements in those components of the CE graph which are maximal with respect to the partial order. (The node set of a digraph is classified into equivalence classes with respect to the equivalence relation such that two nodes are equivalent, i.e. they belong to the same class, if and only if there is a directed path from any one of them to the other. A "strongly connected component" of the digraph is the subgraph consisting of all the nodes of an equivalence class and of all the branches whose end nodes both belong to the class. The relation, defined among the strongly connected components by the stipulation that a component is in the relation to another if and only if there is a directed path from a node of the former component to a node of the latter, is a partial order. There is at least one strongly connected component which is maximal with respect to this partial order.)

The CE graph can be considered to describe the way of propagation of the failure so long as the propagation is explicit on the pattern, i.e. there is no influence through a node with sign 0. Unfortunately, however, if the system has some controlled elements, it may happen that the failure propagates

through a node with sign 0, as is illustrated in the following example.

Example 3. For the water tank system of Fig. 3, the influences among the state variables are represented by the signed digraph of Fig. 4. In case the observed signs of the variables (V_1, F_1, L, V_2, F_2, V_3, F_3) are (+, +, 0, +, +, 0, +), the CE graph for this pattern would be a graph of Fig. 5(a) according to Definition 3. However, it is because the level controller suppresses the

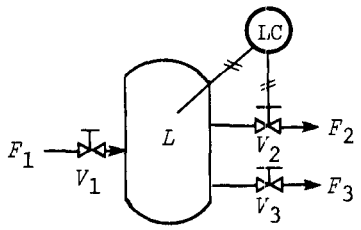


Fig. 3. Another water tank system

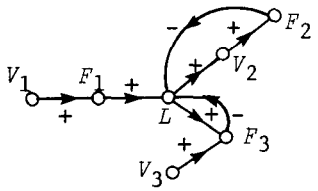
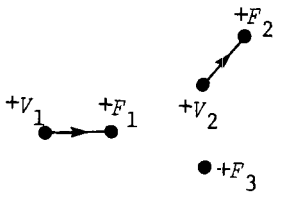
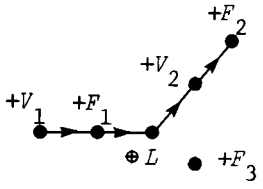


Fig. 4. Signed digraph for the water tank system of Fig. 3



(a) G^*_1



(b) G^*_2

Fig. 5. CE graph for pattern (V_1, F_1, L, V_2, F_2, V_3, F_3) = (+, +, 0, +, +, 0, +) on the signed digraph of Fig. 4

(a) Definition 3 (b) Definition 3'

tendency of the water level L becoming greater than it is normally, that L has a normal value. The actual influences in this case should be described by the digraph G^*_2 of Fig. 5(b). ☒

In order to take account of the special roles of controllers and controlled elements, it is necessary to distinguish some elements of the system as controlled elements, and to extend the formal definitions of a signed digraph, a pattern and a CE graph as follows.

Definition 1'. A *signed digraph* S is the composite concept (G, ψ, C, η) of

(i) a digraph $G = (N, B, \partial^+, \partial^-)$,

(ii) a function $\psi : B \to \{+, -\}$,

and

(iii) a set of controlled nodes $C = \{\mathbf{n}_{\alpha_1}, \mathbf{n}_{\alpha_2}, \cdots, \mathbf{n}_{\alpha_l}\}$ $(\subseteq N)$ to each of which a set of *control-information carrying branches* $\eta(\mathbf{n}_{\alpha_i})$ $(\subseteq \delta^+\mathbf{n}_{\alpha_i})$ $(i = 1, \cdots, l)$ is associated, where $\delta^+\mathbf{n}_{\alpha_i}$ denotes the set of branches whose initial node is $\mathbf{n}_{\alpha_i}$. ☒

Definition 2'. A *pattern* on a signed digraph S is a function $\omega : N \to \{+, 0, -, \oplus, \ominus\}$ such that $\omega(N - C) \subseteq \{+, 0, -\}$. ☒

Definition 3'. Given a pattern ω on a signed digraph S, a node is said to be *valid* if $\omega(\mathbf{n}_\alpha) \neq 0$ and a branch $\mathbf{b}_\kappa$ is said to be *consistent* if $\mathbf{b}_\kappa$ satisfies one of the following five conditions (i) ~ (v):

(i) $\omega(\partial^+\mathbf{b}_\kappa) = \pm$, $\omega(\partial^-\mathbf{b}_\kappa) = \pm$, and $\omega(\partial^+\mathbf{b}_\kappa)\psi(\mathbf{b}_\kappa)\omega(\partial^-\mathbf{b}_\kappa) = +$;

(ii) $\omega(\partial^-\mathbf{b}_\kappa) = \oplus$ and $\omega(\partial^+\mathbf{b}_\kappa)\psi(\mathbf{b}_\kappa) = +$;

(iii) $\omega(\partial^-\mathbf{b}_\kappa) = \ominus$ and $\omega(\partial^+\mathbf{b}_\kappa)\psi(\mathbf{b}_\kappa) = -$;

(iv) $\mathbf{b}_\kappa$ is a control-information carrying branch, $\omega(\partial^+\mathbf{b}_\kappa) = \oplus$ and $\psi(\mathbf{b}_\kappa)\omega(\partial^-\mathbf{b}_\kappa) = +$;

(v) $\mathbf{b}_\kappa$ is a control-information carrying branch, $\omega(\partial^+\mathbf{b}_\kappa) = \ominus$ and $\psi(\mathbf{b}_\kappa)\omega(\partial^-\mathbf{b}_\kappa) = -$.

The subgraph G^* of G which consists of all the valid nodes and all the consistent branches is called the *CE graph* for the pattern ω on the signed digraph S. ☒

In the above definition, sign $\oplus(\ominus)$ might intuitively be interpreted as representing "the state of a variable which would have sign +(-) without control but which is not seen abnormal due to the operation of control".

2. Formulation of the Problem of Locating the Origin of a System Failure

If the observed pattern is a failure pattern, i.e. if there are some nodes with nonzero signs, the CE graph for the pattern can be used to describe the structure of the chain of propagation of the failure, and the problem of locating the origin of the failure is reduced to that of finding the maximal strongly connected components of the CE graph.

However, it is usually the case that some of the signs of nodes cannot be measured or observed due to physical, technical and economical reasons, so that the set of nodes of the signed digraph should be partitioned into two subsets: one (to be denoted by N_M) consisting of *observed nodes* whose signs are measured or observed, and the other (i.e. $N - N_M$) consisting of *unobserved nodes* whose signs are not known.

A method which has been proposed to cope with this situation is found in [2]. By that method we eliminate unobserved nodes from S beforehand and construct a signed digraph S' whose nodes are all observed nodes and whose branches represent indirect influences transmitted through unobserved nodes in S. Then, S' is regarded as the model of the system. Fig. 6 is an illustrative example of the elimination of unobserved nodes.

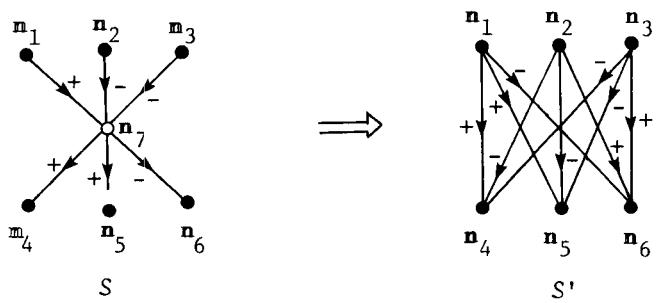


Fig. 6. Example of the elimination of unobserved nodes (● : observed, ○ : unobserved)

However, this method has obvious disadvantages. In fact, the two signed digraphs S and S' of Fig. 6 give different interpretations to a sign pattern on the observed nodes, e.g. to $\omega(\mathbf{n}_i) = +$ ($i = 1, \cdots, 6$). Starting from S we have G^*_1 or G^*_2 of Fig. 7 as the CE graph according as we assume $\omega(\mathbf{n}_7) = +$ or $\omega(\mathbf{n}_7) = -$, whereas from S' we have G^*_3. It is seen that this failure pattern has four or five independent origins on the basis of S on the one hand, and on

the other, it has three independent origins on the basis of S'. This evidences that the elimination of unobserved nodes generally results in loss of information, which might cause the essential structure of the problem to be missed. Moreover, since the elimination of nodes of a graph increases, in general, the number of branches, it is not suitable for the treatment of large graphs from the point of view of computational complexity.

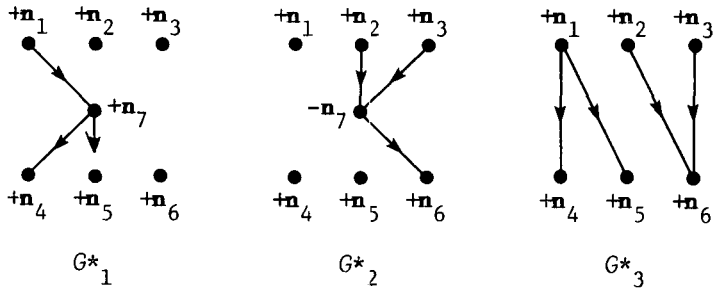


Fig. 7. CE graphs for a sign pattern on the signed digraphs of Fig. 6

Therefore, we shall propose to deal with the given signed digraph and a partial pattern on it (partial in the sense that signs are assigned only to part of the nodes) with no modification, and to restrict the possible locations of the origin of the failure as far as possible. In general, any pattern obtained from a given partial pattern by supplementing in an arbitrary way the signs of the nodes to which the signs are not a priori given, may possibly take place. However, we must exclude from consideration most of those patterns which would not reflect practical situation. In so doing, the following fundamental presumption seems to be natural and it indeed works very effectively.

Presumption of a single origin:

There is a single origin of the system failure. ☒

The CE graph G^* for the pattern corresponding to a system failure satisfying this presumption should be a rooted digraph, which is defined as follows.

Definition 4. We shall call a digraph $G = (N, B, \partial^+, \partial^-)$ a *rooted digraph* if G has a node $\mathbf{n}_\alpha$ such that to every node $\mathbf{n}_\beta$ there is at least one directed path from $\mathbf{n}_\alpha$. (It is well known that a rooted digraph is a graph having only one maximal strongly connected component.) ☒

A "partial pattern" may be formally defined as follows.

Definition 5. Let $S = (G, \psi)$ $(G = (N, B, \partial^+, \partial^-))$ be a signed digraph. A *partial pattern* on S with domain $\tilde{N}$ is a set of signs of the nodes in $\tilde{N}$, where $\tilde{N}$ is a subset of the set N of nodes, i.e. it is a function $\omega^* : \tilde{N} \to \{+, 0, -, \oplus, \ominus\}$. If ω^* is a partial pattern with domain $\tilde{N}$, an *expanded pattern* of ω^* is a pattern $\omega : N \to \{+, 0, -, \oplus, \ominus\}$ such that $\omega|_{\tilde{N}} = \omega^*$. ☒

Then the problem of locating the origin of a system failure under the presumption of a single origin is formulated mathematically as follows.

Problem. Given a signed digraph S and a partial pattern ω^* with domain N_M of observed nodes, to enumerate the expanded patterns of ω^* which make the corresponding CE graphs rooted. ☒

3. An Algorithm for Locating the Origin of a Failure

The solution of the problem formulated in the preceding section may be found in principle by enumerating the CE graphs for all the $3^{|N - N_M|}$ possible expanded patterns and by testing whether each CE graph is rooted or not. However, such a primitive method would require a prohibitively long time if it were carried out on a computer, so that we have to devise a practically more efficient algorithm.

For that purpose, we consider a partition of the set $N - N_M$ of unobserved nodes into two subsets: one being the set N_A of nodes whose signs are tentatively assumed (to be called *assumed nodes*), and the other being the set N_Y of nodes whose signs are not yet assumed (to be called *non-assumed nodes*).

We then consider, for the partial pattern with the set of observed nodes and assumed nodes as the domain, the quasi-CE graph consisting of all those branches which may belong to the CE graph for at least one of the expanded patterns.

Definition 6. Let S be a signed digraph and $\omega^* : N_M \cup N_A \to \{+, 0, -, \oplus, \ominus\}$ be a partial pattern on S with the union of the set N_M of observed nodes and the set N_A of assumed nodes as the domain. A *valid node* is a node $\mathbf{n}_\alpha \in N_M \cup N_A$ with $\omega^*(\mathbf{n}_\alpha) = +, -, \oplus$ or $\ominus$, and a *semi-consistent branch* is a branch which can be a consistent branch for at least one of the expanded patterns of ω^*, i.e. branch $\mathbf{b}_K$ is semi-consistent if $\mathbf{b}_K$ satisfies one of the following two

conditions:

(i) $\partial^+\mathbf{b}_K \in N_V$ and/or $\partial^-\mathbf{b}_K \in N_Y$, and if either $\partial^+\mathbf{b}_K$ or $\partial^-\mathbf{b}_K \in N_M \cup N_A$ then it is valid;

(ii) $\partial^+\mathbf{b}_K \in N_M \cup N_A$, $\partial^-\mathbf{b}_K \in N_M \cup N_A$ and $\mathbf{b}_K$ satisfies one of the conditions (i) ~ (v) of Definition 3' in §1 with ω^* in place of ω.

The subgraph $\tilde{G}$ of G consisting of all the valid nodes and the non-assumed nodes and of all the semi-consistent branches is called the *quasi-CE graph* for partial pattern ω^* on signed digraph S. ☒

Definition 7. Let $\tilde{G}$ be a quasi-CE graph. An *essential component* of $\tilde{G}$ is a strongly connected component containing at least one valid node. An *unessential component* of $\tilde{G}$ is a strongly connected component consisting of non-assumed nodes only. ☒

The following theorem is almost evident but useful for developing a practical algorithm.

Theorem 1. Let $S = (G, \psi)$ be a signed digraph and $\tilde{G}$ be the quasi-CE graph for a partial pattern ω^* with the set of observed nodes and assumed nodes as the domain. Furthermore, let G^* be the CE graph for an arbitrary expanded pattern ω of ω^*. Then, the number $\tilde{m}$ of maximal essential components of $\tilde{G}$ does not exceed the number m^* of maximal strongly connected components of G^*. ☒

For the proof of Theorem 1, we may make use of the following two lemmas which are easily proved.

Lemma 1. Every strongly connected component of a digraph remains to be a component or is divided into several components if some of the branches are removed (i.e. opened). ☒

Lemma 2. Let $G = (N, \mathcal{B}, \partial^+, \partial^-)$ be an acyclic digraph and N' a subset of N. If the set of branches from a node of $N - N'$ to a node of N' is empty, i.e. $\{\mathbf{b}_K \mid \mathbf{b}_K \in \mathcal{B}, \partial^-\mathbf{b}_K \in N', \partial^+\mathbf{b}_K \in N - N'\} = \emptyset$, then there is at least one node of N' which has no branch ending at it. ☒

Proof of Theorem 1: If $\tilde{m} = 0$, the theorem holds. In case $\tilde{m} \geq 1$, let $\mathbb{M}$ be the set of all those nodes of any maximal essential component of $\tilde{G}$ which are valid in G^*. By the definition of an essential component, $\mathbb{M}$ is not empty, and by the definition of a semi-consistent branch, expanding the pattern (i.e.

assigning new signs to nodes) does not give rise to new branches. Therefore, $\mathbf{N}$ is partitioned into strongly connected components of G^* by Lemma 1. Let the partition be $\mathbf{N} = \mathbf{N}_1 \cup \mathbf{N}_2 \cup \cdots \cup \mathbf{N}_k$.

Now, let us consider the digraph G_0 which represents the partial order among the strongly connected components of G^*. Then, there exists no branch connected to the nodes of G_0 corresponding to $\mathbf{N}_i$'s ($i = 1, \cdots, k$) from the other nodes. Therefore, by Lemma 2, there is a node of G_0 corresponding to an $\mathbf{N}_i$ at which no branch ends. Since the strongly connected component of G^* corresponding to this node is maximal, we have proved that, for each maximal essential component of $\tilde{G}$, there exist one or more maximal strongly connected components of G^*, which are obviously disjoint. Hence follows the theorem. Q.E.D.

Corollary 1. Let $\tilde{m}$, G^* be the same as in Theorem 1. If $\tilde{m} \geq 2$, G^* is not a rooted digraph. ☒

By means of this corollary we know that, if $\tilde{m} \geq 2$ for a partial pattern, none of the CE graphs for its expanded patterns can be a rooted digraph, without examining all the expanded patterns.

We shall propose an origin-locating algorithm using Corollary 1 combined with the depth-first search technique, as is outlined in the following.

Origin-locating Algorithm: To begin with, set $N_A = \emptyset$. At each step of the iteration, two cases are possible.

Case A: The quasi-CE graph for the current partial pattern has two or more maximal essential components. In this case, we stop expanding the current partial pattern and examine the possibility of changing the assignment of a sign to one of the assumed nodes.

Case B: The number of maximal essential components of the quasi-CE graph for the current partial pattern equals one or zero. This case is further divided into two subcases.

Case B1: There are one or more non-assumed nodes. In this case we choose one of them to which we assign a sign.

Case B2: There is no non-assumed node. In this case we output the current partial pattern (which is a (nonpartial) pattern) and the CE graph for it, and then go over to the possibility of changing the assignment of a sign to one of the assumed nodes.

We repeat this process until all the possibilities are exhausted. ☒

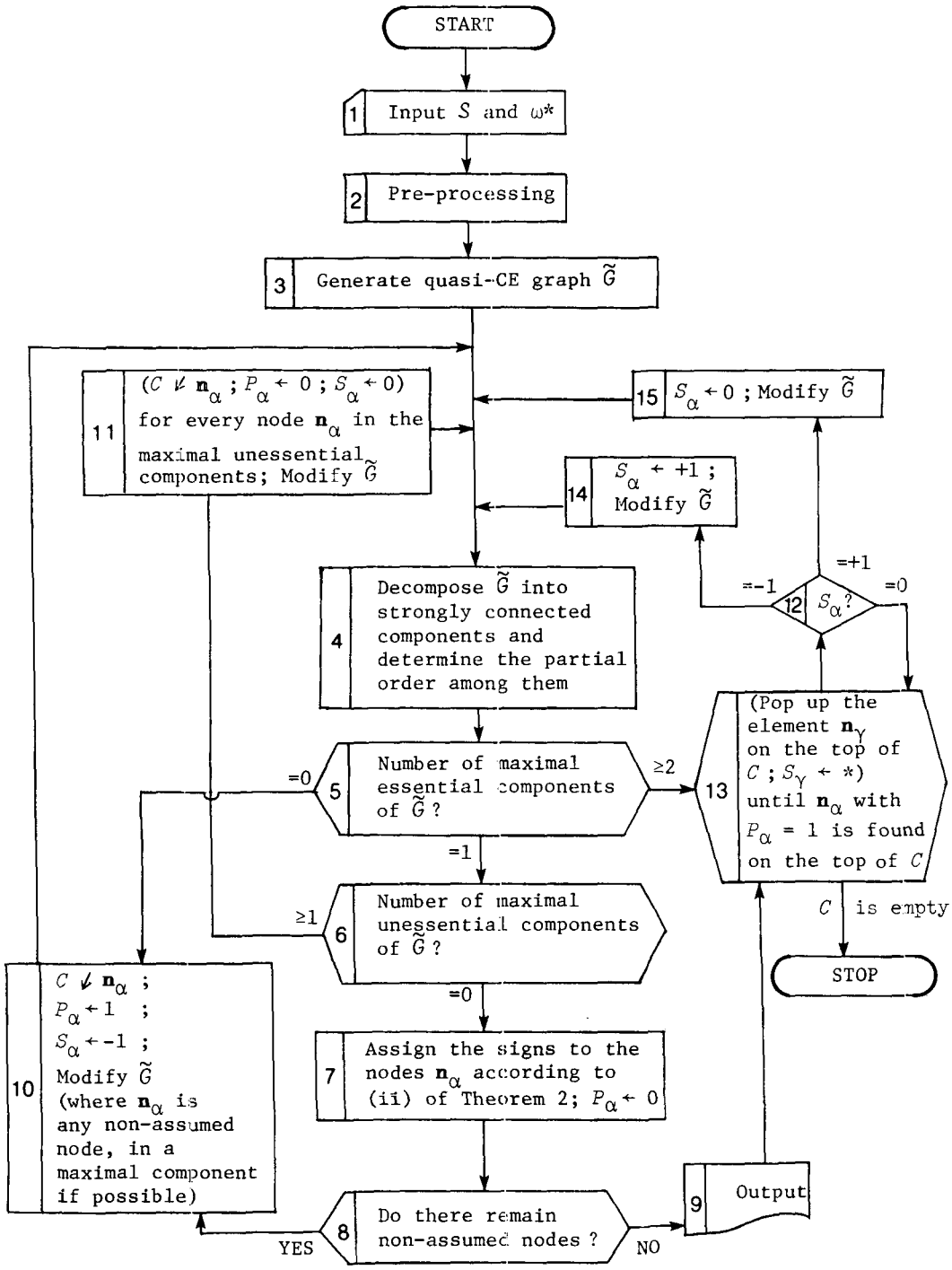


Fig. 8. Outline of the algorithm for locating the origin of a system failure

Since, in an acyclic graph, a node at which no branch ends forms by itself a maximal strongly connected component, we readily have the following theorem (Theorem 2), which is useful for making the algorithm more efficient.

Theorem 2. Suppose that the quasi-CE graph $\tilde{G}$ for a partial pattern on a signed digraph has a single maximal essential component. Then, the following two conditions must be satisfied by any expanded pattern to make the corresponding CE graph G^* a rooted digraph.

(i) Every node of any maximal unessential component of $\tilde{G}$ is assigned sign 0 in the expanded pattern.

(ii) For a strongly connected component of $\tilde{G}$, if there is only one branch $\mathbf{b}_K$ which ends at a node in that component and starts from a node in another component, the deletion of $\mathbf{b}_K$ will make that component maximal. Hence, if one of the ends of $\mathbf{b}_K$ is a valid node and the other is non-assumed node, then the sign of the non-assumed node in the expanded pattern may be determined so as to make $\mathbf{b}_K$ consistent. □

An outline of the "origin-locating algorithm", with the improvements suggested by Theorem 2 incorporated, may be described as the flow chart of Fig. 8, where, for the sake of simplicity, all the controlled nodes are supposed to be observed. The roles played by the stacks and arrays in the flow chart are as follows.

In the "pre-processing" block 2, when the value of a state variable corresponding to a controlled node is within the specified tolerance (i.e. its sign is either 0, ⊕ or ⊖), we open all the branches starting from the node except those carrying control information, and then regard the controlled node as an unobserved one.

C is a stack with the depth equal to the number of nodes. Assumed nodes are pushed down in C each time when a sign is assigned. S as well as P is a one-dimensional array with the size equal to the number of nodes. We put $S_\alpha = *$ if $\mathbf{n}_\alpha$ is a non-assumed node, and S_α is equal to its sign if $\mathbf{n}_\alpha$ is an assumed node.

In blocks 11 and 7, we assign the signs to the relevant nodes according to (i), (ii) of Theorem 2, where we put $P_\alpha = 0$ for those nodes $\mathbf{n}_\alpha$. In block 13, we pop up the nodes in stack C until a node $\mathbf{n}_\alpha$ with $P_\alpha = 1$ (i.e. a node with an "arbitrarily" assigned sign) appears on the top of C.

Block 4 contains a routine to decompose a digraph into strongly connected components. The algorithm proposed by R. E. Tarjan [3] is now regarded as one of the most efficient.

It will not be difficult to see that we can enumerate all the possible sign-assignments by the help of the stack C together with the auxiliary arrays S and P.

Example 4. Let us take up again the system of Fig. 3 in Example 3, which is modelled into the signed digraph S of Fig. 4. Furthermore, let us assume that nodes V_1, L and F_2 are observed, the other nodes being unobserved, and that node L is controlled where control information is carried by the branch to node V_2. Now, suppose pattern $\omega^* : (V_1, L, F_2) \longmapsto (+, 0, +)$ is observed. After the preprocessing block 2, we have the initial quasi-CE graph shown in Fig. 9(a), where node L is regarded as an unobserved node. Since the digraph of Fig. 9(a) has two maximal strongly connected components, i.e. $\{V_1\}$ and $\{V_3\}$, the former being essential and the latter not, node V_3 is assigned sign 0 in block 11, and the quasi-CE graph is modified by removing node V_3 and the branch incident to it. In the resulting quasi-CE graph $\{F_3\}$ is again an unessential maximal component, so that it is removed together with the incident

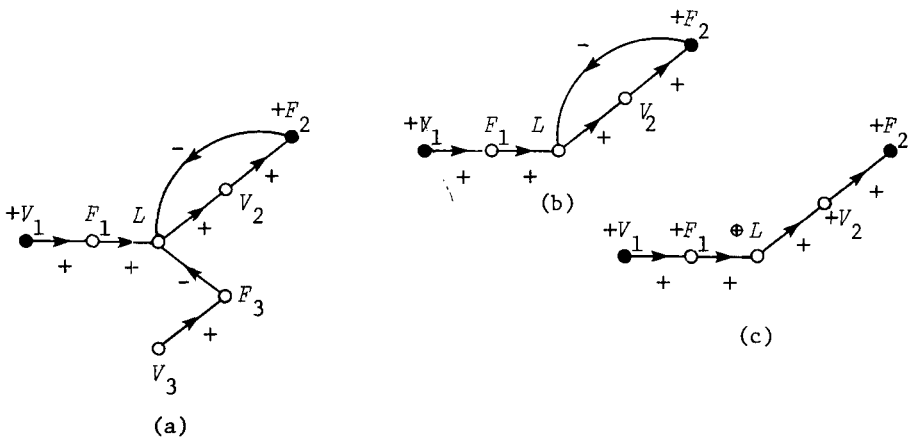


Fig. 9. Example of the algorithm

branch. Then we have the quasi-CE graph of Fig. 9(b). This digraph has only one essential maximal component, so that we apply (ii) of Theorem 2 in block 7 to assign + to node F_1, and then ⊕ to L. Then, the branch from node F_2 to L becomes invalid and is removed from the graph. Thus, by applying (ii) of Theorem 2 again, we have the final CE graph shown in Fig. 9(c), which is unique in this case. The expanded pattern (uniquely determined in this case) is ω : $(V_1, L, F_2; F_1, V_2, V_3, F_3) \longmapsto (+, \oplus, +; +, +, 0, 0)$. Thus, we can conclude that the abnormal phenomenon stems from the unexpected increase in the aperture

of valve V_1.

4. Related Problems

An error-detecting or error-correcting code is famous in the context of error/failure detection and diagnosis. That is a code which is used for improving the reliability of the information transmission through a noisy channel. By taking advantage of a special algebraic structure of the code, *under the assumption that the number of errors is within a specified bound*, we can detect the existence of errors or clarify their locations.

Our problem has a common feature with an error-detecting (-correcting) code in that the location of the origin of a system failure is to be found on the basis of the information obtained by some observation (i.e. a pattern of signs of observed nodes) *under the assumption of a single origin of failure*. But there is a basic difference between the error-detecting (-correcting) code and our problem. In the former, it is possible --- and it is the most important point of the theory --- to design an artificial structure which enables us to detect (correct) errors, whereas, in the latter, the structure of the system as well as the observability/unobservability of the signs of nodes are a priori given.

A fault diagnosis of a logical circuit is also well known. The location of fault is determined by means of a combination of many tests (each of which is an input-output sequence pair) [4]. Thus, the problem of fault diagnosis of a logical circuit and our problem have the same purpose, i.e. to determine the origin of a failure in a *given* system. However, there is much difference between the two problems. In our problem, only the information given in the form of a pattern of the signs of observed nodes is available when a failure takes place, whereas, in the diagnosis of a logical circuit, arbitrary signal sequences (which are prepared especially for the purpose of diagnosis) may be input to the system in order to obtain useful information.

5. Discussions on the Problems to be Solved

In this paper we presented the concept of a signed digraph and a pattern on it as a mathematical model for describing roughly a system and its state, and formulated the problem of locating the origin of a system failure in terms of those concepts. A practical algorithm for the problem was also proposed.

The present formulation of the model is motivated through an attempt to establish a systematic approach to the automatic diagnosis of the failures of chemical plants. However, the model seems to be applicable to a wider variety of engineering as well as social systems.

There remains, of course, much to be further developed both from the mathematical and the practical points of view.

Mathematically, the present version of origin-locating algorithm is rather primitive. For example, a part of a chemical plant was modelled into a digraph with 21 nodes and 62 branches, of which 6 nodes are observed and 3 nodes are controlled. The origin-locating algorithm generated about 20,000 quasi-CE graphs and examined their connectivity. It took about 20 minutes on FACOM 230/45 operating under FORTRAN IV monitor.

The necessary time will increase very rapidly, i.e. exponentially, as the size of the graph, especially the number of unobserved nodes and controlled nodes, increases. However, we can introduce various devices similar to those enunciated in Theorem 2 to greatly cut down the number of quasi-CE graphs to be examined. Designing such devices will afford interesting and useful research subjects in graph theory. In fact, by adding a few such devices to the algorithm, we could solve the same problem in less than 10 seconds. For a given specific system, the more of its special structures we take advantage of, the more devices shall we be able to find to speed up the algorithm.

There will be a number of problems when we make a model of a real system. For example, an implicit relation such as $f(x, y, z) = 0$ among state variables

(a) (b)

Fig. 10. Example of the digraphical representation of an implicit relation

cannot be represented in the unique way by the branches which connect the nodes representing variables x, y, z. However, if the signs of partial derivatives of f with respect to the variables are known, say, $f_x > 0$, $f_y > 0$ and $f_z < 0$,

it may be possible to represent the implicit relation by a bipartite graph with a dummy node as shown in Fig. 10(a), and then by a signed digraph as shown in Fig. 10(b).

In the case that the method is applied to a continuous system such as a chemical process, the influence relations and the values of state variables are to be quantized into two or three levels. A standard method should be looked for for the quantization.

It is clear that, the more nodes are observed, the smaller will be the part within which the origin of failure is confined and the faster will the algorithm run. However, in practice, the number of observed nodes is limited by physical, technological and economical reasons. Here arises the problem of establishing a criterion according to which observed nodes are to be distributed. This leads us to a problem of synthesis of a system in contrast with the problem of analysis considered in this paper.

The authors are trying to implement the method presented in this paper in an actual chemical plant, where they are finding practical solutions to the problems discussed in this section. The theoretical results, as well as the practical, obtained in the course of the trial will be published elsewhere before long.

The authors thank the referees for their valuable comments and suggestions, by which the manuscript of the paper was substantially improved.

This work was supported in part by the Grant in Aid for Scientific Research of the Ministry of Education, Science and Culture of Japan.

References

[1] Iri, M.: *Network Flow, Transportation and Scheduling --- Theory and Algorithms*. Academic Press, New York, 1969. See also: Iri, M.: Theory of Graphs and Its Applications [I]-[V] (in Japanese), *Journal of the Institute of Electronics and Communication Engineers of Japan*, Vol.54, No.12 - Vol.55, No.5 (Dec. 1971 - May 1972).

[2] Andow, P. K., and Lees, F. P.: Process Computer Alarm Analysis: Outline of a Method Based on List Processing. *Transactions of the Institution of Chemical Engineers*, Vol.53 (1975), 195-208.

[3] Tarjan, R. E.: Depth-first Search and Linear Graph Algorithms. *SIAM Journal on Computing*, Vol.1, No.2 (June 1972), 146-160.

[4] Chang, H. Y., Manning, E. G., and Metze, G.: *Fault Diagnosis of Digital Systems*. Wiley-Interscience, 1970.

Masao IRI: Department of Mathematical Engineering and Instrumentation Physics, Faculty of Engineering, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan 113.

References added in proof

[5] Iri, M., Aoki, K., O'Shima, E., and Matsuyama, H.: An Algorithm for Diagnosis of System Failures in the Chemical Process. *Computer and Chemical Engineering* (to appear).

[6] Umeda, T., Kuriyama, T., O'Shima, E., and Matsuyama, H.: Graphical Approach to Causes and Effects Analysis of Chemical Processing Systems. *The 12th European Symposium on Computer Applications in Chemical Engineering*, Montreux, April 1979.