Malfunction Diagnosis Using Quantitative Models with Non-Boolean Reasoning in Expert Systems

An approach to chemical plant fault diagnosis is presented that utilizes patterns of violation and satisfaction of the quantitative constraints governing the process. Process knowledge consists of a list of the operational constraints on the plant together with sufficient conditions for violation of each constraint. Interpretation of the pattern of constraint violations is treated by Boolean and non-Boolean techniques. It is shown that non-Boolean reasoning techniques increase the stability and sensitivity of the diagnosis in the presence of noise. The techniques introduced in this paper are easily implemented in rule-based expert systems using certainty factors.

M. A. Kramer
Department of Chemical Engineering
Massachusetts Institute of Technology
Cambridge, MA 02139

Introduction

In an operating chemical plant, product quality is maintained by monitoring process variables and controlling their fluctuations within a desired range. When operating conditions vary outside these design limits, not only is product quality in jeopardy, but if left uncorrected these variations could result in a catastrophic event such as an explosion, fire, or the release of toxic chemicals. Diagnosis of process malfunctions is a difficult task for process operators. Although well trained in standard operating procedures, operators may have difficulty handling unanticipated events and low-probability failures. Because time constraints are critical, hesitation as well as inappropriate action could lead to disaster. This paper presents a method of automated malfunction diagnosis intended to help operators determine the presence and identity of process faults.

Various methods of automated fault diagnosis have been proposed. Diagnosis by cause-and-effect analysis using patterns of process alarms is discussed by O'Shima and coworkers (Iri et al., 1979; Tsuge et al., 1985; Shiozaki et al., 1985). A related technique has been proposed for alarm analysis (Andow and Lees, 1975; Andow, 1980; Lees, 1983). Fault trees have been used by Martin-Solis et al. (1982) and Yoon (1982). These methods are nonquantitative and therefore are not highly sensitive detectors of violations of process mass or heat balances.

Quantitative diagnostic methods based on filtering and estimation techniques have been discussed by many authors, and only a small fraction can be cited in this space. Stanley and Mah (1977) use a Kalman filter with a quasi-steady state process model for data rectification and for detection of leaks and measurement biases. Watanabe and Himmelblau (1984) apply an extended Kalman filter to detect parameter variations indicative of process faults. The same authors apply a nonlinear estimator to diagnosis of a chemical reactor (Watanabe and Himmelblau 1983a,b). Recent advances in fault detection by estimation techniques are summarized by Isermann (1984). Particularly when dynamic models are used, these techniques require extensive modeling and computation and are not well suited for monitoring and diagnosis at the full-plant level.

Redundancy between process measurements can be used to improve the information content of signals and detect significant deviations from process material and energy balances. Mah et al. (1976) apply a constrained least-squares approach to estimate unmeasured flows in process networks and minimize the differences between process measurements and estimated values subject to process material balances. Leak and measurement error detection is accomplished by testing each mass balance for significant violations. The source of the gross error is identified by a topological procedure after classification of balances into sets of faulty and nonfaulty balances. Romagnoli and Stephanopoulos (1981) present a similar analysis that is coupled with a method of serial elimination of suspect measurements. Improved statistical methods for detecting gross errors in process measurements have been suggested by Mah and Tamhane (1982) and Madron (1985).

Another approach to fault diagnosis involves expert systems. Expert systems have been applied to diagnosis problems in several domains, for example, in medical diagnosis (Shortliffe, 1976; Pople, 1982; Patil et al., 1981), and in electronic and mechanical system diagnosis (Davis, 1984; Genesereth, 1984; Fink et al., 1985). In the process domain, examples are given by Kumamoto et al. (1984), Chester et al. (1984), Davis et al. (1985), Ungar (1985), Andow (1985), and Beazley (1986). Expert systems allow the accumulated experience, judgment, and heuristics of process engineers and operators to be incorporated into automated reasoning systems. Application of this expert knowledge in real time by direct access to plant measurements in theory allows for improved and more consistent plant operation in spite of personnel turnover, lapses in human attention, and the like. Computational environments for the application of expert knowledge in real time to chemical processes are provided by PICON (Moore et al., 1985) and by ONSPEC (Heuristics, Inc., 1985). Field tests with expert systems have been conducted at Texaco and Exxon Chemicals (Moore, 1985), and at DuPont (Lamb et al., 1985).

In the medical domain, expert systems are typically based on the experience of one or more doctors recognized as experts in a certain class of diseases. In contrast to this approach, expert systems based solely on experience are not ideal in chemical plant fault diagnosis. Experts may not be as readily available or as highly trained. Many faults needing to be diagnosed may never have been experienced, and for new or recently retrofitted plants, there may be no applicable experiential knowledge. The experiential approach requires that most if not all of the knowledge be developed from scratch for each new application. This is a critical problem because the number of rules required for large plants may be as high as 10,000 to 100,000 (Moore and Kramer, 1986). Finally, the experiential approach is most appropriately applied to unstructured problems where the theoretical or conceptual basis for reasoning is not well understood. In the chemical engineering environment, a large fraction of the knowledge is structured, and physical models based on thermodynamics, heat, mass and momentum transfer, kinetics, and process chemistry can be incorporated into the diagnosis.

In recognition of these difficulties, the present paper focuses on model-based approaches to fault diagnosis. Nonetheless, it is recognized that experiential knowledge will play a key role in actual applications of expert systems to fault diagnosis and other areas of process operations. Therefore, the current work emphasizes the translation of model-based diagnostic techniques into sets of rules which can be incorporated into a larger expert system that includes experiential rules. In fact, the diagnostic technique in the present work is intended only as one element in a three-part approach to diagnosis which includes causal search and experiential knowledge as the remaining components (Kramer and Palowitch, 1985).

In the remainder of this paper, we present the quantitative method of fault diagnosis, first in the framework of Boolean logic, followed by the introduction of non-Boolean reasoning techniques. Using two non-Boolean techniques, the governing equations method is translated into a set of expert system rules. A comparison between these methods and the Boolean approach is then developed, using a simulation example.

The Method of Governing Equations

The material and energy balances, rate equations, and equilibrium relations on a process provide a set of constraints on the values of process variables. Significant violations of these constraints are indicative of process faults. The method of governing equations is based on associating each quantitative constraint on a process with the set of faults that are sufficient to cause violation of the constraint. For example, let $F_1 - F_2 = 0$ represent the mass balance for flow into and out of a processing unit. If the lefthand side of this expression is significantly less than zero, then we establish the inference (F_1-SENSOR-FAILS-LOW) $\vee$ (F_2-SENSOR-FAILS-HIGH). If the expression is significantly greater than zero, we infer (F_1-SENSOR-FAILS-HIGH) $\vee$ (F_2-SENSOR-FAILS-LOW) $\vee$ (SYSTEM-LEAK). Importantly, these conditions are the *only* explanations for violation of the constraint (assuming no leaks into the system). Logical combination of the inferences drawn from the full set of process constraints yields the pertinent diagnosis.

Analysis of the balances by comparison to process data requires constraints in which all quantities are either measured or nominally fixed. Although in most processes there will be unmeasured as well as measured variables, the techniques of nodal aggregation (Mah et al., 1976) or output set assignment (Romagnoli and Stephanopoulos, 1980) can be used to produce a set of constraints in which all quantities are measured.

In formal notation, the method of governing equations can be expressed as follows. Let C_i^+, C_i^- and C_i^0 be the conditions for positive and negative constraint violation and constraint satisfaction, respectively.

$$\begin{aligned} C_i^+ &\leftrightarrow (C_i > \text{tol}_i) \\ C_i^0 &\leftrightarrow (|C_i| \le \text{tol}_i), \quad i = 1, \dots \text{NC} \\ C_i^- &\leftrightarrow (C_i < -\text{tol}_i) \end{aligned} \tag{1}$$

It is assumed for simplicity that significant violations of each constraint can be expressed by a fixed tolerance applied to each constraint. This assumption will be relaxed in a subsequent section. Let F be the set of all possible faults, whose members we shall call f. We define the set of faults that are sufficient to cause violation of the ith constraint as follows:

$$\begin{aligned} (\forall f)(f \rightarrow C_i^+) \in H_i^+ \\ (\forall f)(f \rightarrow C_i^-) \in H_i^- \end{aligned} \tag{2}$$

Let F^* be the set of faults actually present in the plant. The critical assumption of the method is that no constraint is simultaneously affected by two or more faults having competing effects, i.e.,

$$[(F^* \cap H_i^+) = \phi] \vee [(F^* \cap H_i^-) = \phi], \quad i = 1, \dots NC \tag{3}$$

where ϕ is the empty set. Define the condition of the plant to be C^*, where $C_i^* = C_i^+, C_i^-$, or C_i^0 depending on whether the ith constraint is violated high or low, or satisfied. Similarly, let H_i^* be the fault set activated by the condition of the ith constraint, as follows:

$$\begin{aligned} (C_i^* = C_i^+) &\rightarrow (H_i^* = H_i^+) \\ (C_i^* = C_i^0) &\rightarrow [H_i^* = {}^{\sim}(H_i^+ \cup H_i^-) \equiv H_i^0] \\ (C_i^* = C_i^-) &\rightarrow (H_i^* = H_i^-) \end{aligned} \tag{4}$$

Note that if the ith constraint is normal, then none of the faults that are sufficient to cause violation of the constraint can be present. Now let the elements of H_i^* be enumerated as follows:

$$H_i^* = \{h_{i1}, h_{i2}, \ldots h_{il}\}$$

If we define

$$\underline{H}_i^* \leftrightarrow h_{i1} \vee h_{i2} \vee \ldots \vee h_{il},$$

then the implication of the ith constraint is $C_i^* \rightarrow \underline{H}_i^*$. The overall implication of all constraints is formed by conjoining (with "and") the implications of the individual constraints, resulting in the diagnosis:

$$C^* \rightarrow \underline{H}_1^* \wedge \underline{H}_2^* \wedge \ldots \wedge \underline{H}_{NC}^*, \tag{5}$$

where NC is the number of constraints. Equation 5 applies for both single and multiple faults, under the restrictions of Eq. 3.

A special solution of Eq. 5 exists for the case of a single fault. Viable single-fault hypotheses are those that account for all violated constraints, and therefore lie in the intersection of the H_i^*. The set S_1 of single-fault hypotheses is therefore:

$$S_1 = (H_1^* \cap H_2^* \cap \ldots \cap H_{NC}^*) \tag{6}$$

For the remainder of this paper, only the case of single faults will be treated.

This method can be viewed as a generalization of the method of Mah et al. (1976) to faults other than leaks and sensor failures, and an improvement in the sense of providing an explicit formula rather than an algorithmic approach to the diagnosis. Additionally, use of directional information results in higher resolution than that possible based on incidence alone. Suppose there are two violated constraints, $F_1 + F_2 - F_3 = 0$ and $F_1 - F_2 = 0$. Based solely on the incidence of F_1 and F_2 in the violated constraints, sensor failure in F_1 or F_2 is suggested. The current method concludes F_1 sensor failure if both constraints are violated in the same direction, and F_2 sensor failure if the constraints are violated in opposite directions.

Example 1

Table 1 lists possible faults on violation of a certain set of constraints. Suppose that constraint 1 is high and constraint 2 is low. Then the single fault diagnosis is $S_1 = \{A, B\} \cap \{A, D\} = \{A\}$. If constraint 1 is normal and constraint 2 is low, then $S_1 = {\sim}\{A, B, C\} \cap \{A, D\} = \{D\}$.

Table 1. Fault Table for Examples 1, 5, 6, and 7

	H^+	H^-
Constraint 1	A, B	C
Constraint 2	B	A, D

Another problem with Boolean classification of constraints is that only two values, true and false, are recognized. This does not reflect the reality that in most cases a diagnosis cannot be rendered with complete certainty. Alternate approaches that recognize the role of uncertainty are required.

In this section, we introduce two such methods, Shafer's mathematical theory of evidence (Shafer, 1976) and fuzzy set theory (Zadeh, 1965). In these methods, incremental changes in the plant state result in incremental changes in degrees of belief of fault hypotheses. This eliminates the noise effects that become dominant when constraints are near threshold values. Also, a ranking of probable faults is obtained. We begin this section with a brief overview of techniques for non-Boolean reasoning.

Application of Non-Boolean Inference Techniques

The previous derivation of the method of governing equations relies on precise classification of constraints into the categories C^+, C^-, and C^0. A single misclassification radically alters the diagnosis, perhaps eliminating an otherwise viable hypothesis or introducing spurious candidates. At threshold values, the diagnosis is infinitely sensitive to incremental changes in the plant state, an effect we call diagnostic instability. For instance, in example 1, if constraint 1 is near the threshold between normal and high, measurement noise will cause the diagnosis to fluctuate between A and D. This instability can occur *regardless of the power of the statistical method used to classify the constraints,* as long as the constraints are classified into disjoint sets.

Bayesian inference

This is a statistical approach to reasoning under uncertainty, dealing with two types of probabilities. The first is the unconditional probability, $P(A)$, which gives the *a priori* probability of A in the absence of evidence. The second type of probability is conditional probability, $P(A|B)$, which is the probability of A given B. The conditional probability of fault f under the set $S = \{s_1, s_2, \ldots\}$ of observed symptoms is:

$$P(f|S) = P(f) * \frac{P(s_1|f)}{P(s_1)} * \frac{P(s_2|f)}{P(s_2)} * \ldots \tag{7}$$

There are several assumptions underlying Eq. 7, the most restrictive being the assumption of independence of symptoms, which states that the probability of one symptom is unaffected by the actual occurrence of other symptoms. In process applications, this assumption is probably erroneous. Further, the unconditional probabilities for faults and symptoms are not readily available. Therefore, it is doubtful that the Bayesian approach is useful in diagnosing process plants. Charniak and McDermott (1985) present an account of Bayesian inference and discuss its application in expert systems.

Fuzzy logic

Fuzzy logic, proposed by Zadeh (1965), uses the concept of membership grade to express variable degrees of inclusion of items in sets. A fuzzy set X is a set of ordered pairs:

$$X = \{(x_1, \chi_1), (x_2, \chi_2), \ldots\}$$

where χ_i is a number of the interval [0, 1] representing the grade of membership of x_i in X, with the ends of this interval representing no membership and full membership, respectively. The Boolean set operations of union and intersection have fuzzy counterparts as follows (Kandel, 1982):

$$X \cup X' = \{[x_1, \max(\chi_1, \chi_1')], [x_2, \max(\chi_2, \chi_2')], \ldots\} \tag{8a}$$

$$X \cap X' = \{[x_1, \min(\chi_1, \chi_1')], [x_2, \min(\chi_2, \chi_2')], \ldots\} \tag{8b}$$

where the x_i include all elements of X and X'. Thus, the degree of membership of an element x in the union of X and X' is the maximum degree of membership of x in the two sets; the membership grade in the intersection is the minimum membership grade of x in X and X'. Since this is a set-based framework, it is a natural means for introducing a non-Boolean character to the governing equations method.

Confirmation theory

Bayesian theory asserts that any evidence supporting a hypothesis must also equally deny the negation of the hypothesis. Hempel (1965) questions the validity of this assumption with respect to human reasoning, leading to an alternate means of uncertain inference called confirmation theory. A model of inexact reasoning based on confirmation theory (Shortliffe and Buchanan, 1975) serves as the basis for the expert system MYCIN (Shortliffe, 1976). MYCIN uses certainty factors (CF's) to quantify the degree of confirmation of hypotheses, which are manipulated according to the following rules:

1. The combined CF of the conjunction of a set of premises is the minimum CF of the individual premises.
2. The combined CF of the disjunction of a set of premises is the maximum CF of the individual premises.
3. The CF for the consequent of a rule is the overall CF of its premise times the CF of the rule.
4. The CF for a hypothesis produced as the conclusion of one or more rules is the bounded sum of the CF's produced by the rules yielding that conclusion. [The bounded sum of two numbers a and b in the interval [0, 1] is $a \oplus b = a + (1 - a)^*b$.]

It will be shown subsequently that in the context of the governing equations method applied to single faults, the MYCIN approach is equivalent to the fuzzy set approach.

Mathematical theory of evidence

Like the fuzzy set approach, this approach by Shafer (1976) is well-suited to the current problem since it is based on sets. Additionally, it resembles the confirmation theory approach in that the probability of a hypothesis is not necessarily equal to one minus the probability of the negation of the hypothesis. Additionally, the method reduces to both the Boolean and Bayesian approaches when evidence fits certain forms. Thus, the Boolean formulae of the previous section are retained as a special case of the theory introduced in this section. Because of the many attractive features of this method, we utilize this framework as the basis for most of the subsequent developments in this paper.

In the theory of evidence, the likelihood of a proposition is represented as an interval $[s(\mathrm{A}), p(A)]$, a subset of the interval [0, 1]. The first parameter, $s(A)$, represents the evidential support for A, while $p(A)$ represents the plausibility of the proposition, or the degree to which contradictory evidence is lacking. Specifically, the plausibility $p(A)$ is defined as:

$$p(A) = 1 - s(\tilde{}A) \tag{9}$$

where $s(\tilde{}A)$ is the evidential support for the proposition $\tilde{}A$. An alternate interpretation of the evidential interval is that the probability of A is bounded between $s(A)$ and $p(A)$. The uncertainty of A is given by $u(A) = p(A) - s(A)$. If $u(A) = 0$ for all propositions of interest, the Bayesian theory results.

As outlined by Garvey et al. (1981), this representation of partial truth is demonstrated by the following examples:

$A[0, 1] \rightarrow$ No information exists regarding A
$A[0, 0] \rightarrow$ A is false
$A[1, 1] \rightarrow$ A is true
$A[0.3, 1] \rightarrow$ Evidence partially supports A
$A[0, 0.7] \rightarrow$ Evidence partially supports $\tilde{}A$
$A[0.3, 0.7] \rightarrow$ Partial support for both A and $\tilde{}A$; the probability of A is between 0.3 and 0.7, with uncertainty of 0.4

Propositions in the theory of evidence are represented as subsets of the set of all relevant propositions, θ, called the frame of discernment. In the fault diagnosis application, θ includes all faults, together with the state of normal operation (equivalent to the negation of all faults).

The evidential intervals $[s(A), p(A)]$ are derived from a basic probability mass distribution (BPMD), which is the basic manipulated quantity in the theory. The BPMD distributes a unit of belief over the set of propositions in a domain. In particular, the basic probability mass (BPM) $m\langle A\rangle$ represents the portion of the unit of belief attributable to the proposition A, where A can be any subset of θ. Belief ascribed directly to θ represents the residual belief that cannot be ascribed to any subset of θ on the basis of available evidence, which in effect introduces uncertainty into the diagnosis. The support for a proposition A, $s(A)$, is the sum of beliefs attributed to A and all subsets of A:

$$s(A) = \Sigma\, m_i\langle A_i\rangle, \quad A_i \subset A \tag{10}$$

From Eq. 9, the plausibility of a proposition is given by one minus the belief accorded $\tilde{}A$ and all subsets of $\tilde{}A$, and therefore:

$$p(A) = 1 - \Sigma\, m_i\langle B_i\rangle, \quad B_i \subset \tilde{}A \tag{11}$$

The set $\tilde{}A$ is the set θ with elements of A removed. The evidential intervals for the negation of a hypothesis is given by $\tilde{}A[1 - p(A), 1 - s(A)]$, which follows from Eq. 9.

Example 2

Consider the frame of discernment $\theta = \{A, B, C\}$. Suppose belief is distributed according to the BPMD $m_1\langle A, B, \theta\rangle = \langle 0.3, 0.5, 0.2\rangle$. The evidential intervals are then given by $A[0.3, 0.5]$, $B[0.5, 0.7]$, $C[0, 0.2]$, $\tilde{}A[0.5, 0.7]$, $\tilde{}B[0.3, 0.5]$, $\tilde{}C[0.8, 1.0]$.

Example 3

Suppose under the same frame of discernment as the previous example, $m_2\langle A, \tilde{}A, B, \tilde{}B\rangle = \langle 0.1, 0.3, 0.4, 0.2\rangle$. Then the evidential intervals are $A[0.1, 0.3]$, $B[0.4, 0.7]$, and $C[0, 0.5]$. The plausibility of A, for example, is determined from one minus the BPM of $\tilde{}A$ and the subsets of $\tilde{}A$, i.e., $1 - m_2(\tilde{}A) - m_2(B) - m_2(C)$. Note that $\tilde{}A \equiv \theta\,\tilde{}A = \{B, C\}$.

In a given problem there may be several sources of information contributing degrees of belief to various propositions under a common frame of discernment. Dempster's rule of combination (Shafer, 1976) provides a method of combining BPMD's derived from independent knowledge sources. For multiple knowledge sources, the sum is commutative and therefore insensitive to the order in which knowledge sources are combined.

Dempster's rule of combination for combining the basic probability masses (BPM's) of two knowledge sources m_1 and m_2 is given by the following:

$$m\langle C\rangle = \Sigma\, m_1\langle A_i\rangle * m_2\langle B_j\rangle/(1 - k),$$

where $A_i \cap B_j = C$,

$$k = \Sigma\, m_1\langle A_i\rangle * m_2\langle B_j\rangle \tag{12}$$

where $A_i \cap B_j = \phi$.
In other words, the BPM donated to the intersection of A_i and B_j is the product of the BPM's of A_i and B_j. The factor $(1 - k)$ is a normalization factor that keeps the total belief equal to unity. This adjustment is necessitated by the presence of propositions in m_1 and m_2 whose intersection is empty, resulting in the donation of a portion of the total belief to the empty set.

Example 4

Two knowledge sources m_1 and m_2 bear on propositions in $\theta = \{A, B, C\}$ with BPMD's given in examples 2 and 3. Calculation of the combined BPMD is visualized in Figure 1. The BPM contributed to the empty set is $k = 0.1 * 0.5 + 0.3 * 0.3 + 0.4 * 0.3 + 0.2 * 0.5 = 0.36$. The BPM contributed to A is $m\langle A\rangle = (0.1 * 0.2 + 0.1 * 0.3 + 0.2 * 0.3)/(1 - 0.36) = 0.17$. Similarly, the BPM's for B, $\tilde{}A$, and $\tilde{}B$ are 0.67, 0.094, and 0.063, respectively. The evidential intervals implied by the combined BPMD are: $A[0.17, 0.24]$, $B[0.67, 0.77]$, $C[0, 0.16]$.

Dempster's rule can be used to process the information deriving from the governing equations method. The ith constraint distributes a unit of belief among the fault sets H_i^+, H_i^-, and H_i^0. The individual BPMD's can be combined into an overall BPMD that can then be used to determine the evidential interval for each fault. Before this procedure can be outlined in detail, however, it must be determined how the constraints distribute belief among the fault sets.

Assignment of the Basic Probability Masses

Let us first examine the conventional means of classification of constraints into the categories high, low, and normal. Let ϵ_i be the residual of the ith constraint equation. ϵ_i is assumed to be a normally distributed random variable of zero mean and variance σ_i^2. This variance can be determined experimentally, or it can be estimated from the variances of the measured quantities in the constraint, using standard statistics. The chi-squared distribution $P(\chi_c^2)$ gives the probability that $\chi^2 = \epsilon_i^2/\sigma^2$ exceeds χ_c^2. A constraint is considered to be high or low if χ^2 exceeds the value of χ_c^2 for a prespecified level of significance, say $P(\chi_c^2) = 0.1$ (90% confidence). In other words, the belief assigned to C_i^0 is one if $\chi^2 < \chi_c^2$, and zero outside this range. This belief is depicted in Figure 2.

This method is a reasonable basis for selection of the tolerances tol_i in the Boolean approach. This is the same criterion used by Mah et al. (1976), and similarly by Romagnoli and Stephanopoulos (1981) prior to their topological analyses. Additionally, since we are analyzing each constraint separately, the measurement test of Mah and Tamhane (1982) also reduces to this test function.

As stated previously, the Boolean classification of constraints leads to the condition of diagnostic instability in the presence of

Θ 0.2	A 0.02	BvC 0.06	B 0.08	AvC 0.04
B 0.5	Φ 0.05	B 0.15	B 0.20	Φ 0.10
A 0.3	A 0.03	Φ 0.09	Φ 0.12	A 0.06
	A 0.10	BvC 0.30	B 0.40	AvC 0.20

Figure 1. Combination of BPMD's for example 4.

measurement noise: incremental changes in plant operating conditions result in nonincremental changes in the beliefs associated with diagnoses. If step functions are used to describe beliefs, diagnoses will always be unstable, regardless of the statistical criterion used to classify constraints. It is therefore desirable to smooth the belief function indicated in Figure 2. The general shape of this smoothed belief function should be sigmoidal, as indicated by rounding the corners of the step function, shown as the hatched lines in Figure 2. A functional form that achieves this smoothing is

$$b_i = (1 - u_i)\frac{x_i^n}{1 + x_i^n},$$
$$x_i = \epsilon_i^2/(\sigma_i^2 \cdot \chi_c^2), \tag{13}$$

where $b_i = b_i(\epsilon_i)$ is the belief function for the ith constraint. Equation 13 uses the adjustable parameter n as the degree to which the step function is smoothed; $n \to \infty$ corresponds to no smoothing, and $n = 0$ to complete smoothing (b_i = constant). When $n \to \infty$, the theory of evidence reduces to the Boolean diagnosis. The factor $(1 - u_i)$ permits the introduction of uncertainty into the belief function when the reliability of the information deriving from the constraint is less than unity.

The evidential intervals based on the belief function of Eq. 11 are as follows:

$$H_i^+[b_i, b_i + u_i],\ H_i^-[0, u_i],\ H_i^0[1 - b_i - u_i, 1 - b_i] \text{ if } \epsilon_i > 0,$$
$$H_i^+[0, u_i],\ H_i^-[b_i, b_i + u_i],$$
$$H_i^0[1 - b_i - u_i, 1 - b_i] \text{ if } \epsilon_i < 0, \tag{14}$$

These intervals can be interpreted as follows. If the constraint residual is greater than zero, the probability that the constraint is high is at least b_i and at most $b_i + u_i$. The probability that the constraint is low is between zero and u_i. The probability that the constraint is normal is at most $1 - b_i$ (complementing H_i^+) with

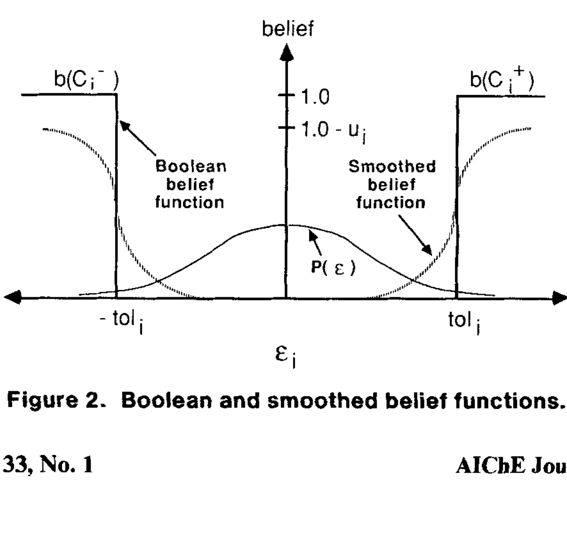

Figure 2. Boolean and smoothed belief functions.

uncertainty u_i. Corresponding inferences are drawn if the residual of the constraint is less than zero.

Consistent with the assignment of belief in Eq. 14, the following basic probability masses are assigned to fault sets H_i^+, H_i^-, and H_i^0:

$$m\langle H_i^+, H_i^-, H_i^0, \theta\rangle = \langle b_i, 0, 1 - b_i - u_i, u_i\rangle, \quad \epsilon_i > 0$$
$$\langle 0, b_i, 1 - b_i - u_i, u_i\rangle, \quad \epsilon_i < 0 \quad (15)$$

Note that the uncertainty is introduced by assigning the mass u_i directly to θ. Essentially, this means that u_i supports all hypotheses, and cannot be attributed to any particular subset of θ.

Example 5

Consider again the fault table, Table 1. The frame of discernment is $\theta = \{A, B, C, D, \$\}$, where \$ stands for fault-free operation. Suppose b_1 and b_2 equal 0.8 and 0.7, respectively, with $\epsilon_1 > 0$ and $\epsilon_2 < 0$. The uncertainties associated with the constraints are assumed to be 0 and 0.2, respectively. From Eq. 15,

$$m_1\langle A \vee B, C, \bar{}(A \vee B \vee C), \theta\rangle = \langle 0.8, 0, 0.2, 0\rangle$$
$$m_2\langle B, A \vee D, \bar{}(A \vee B \vee D), \theta\rangle = \langle 0, 0.7, 0.1, 0.2\rangle$$

Combination of these BPMD's is depicted in Figure 3. The mass assigned to the empty set is $k = 0.08$. From Eq. 10,

$$m\langle A, B, C, D, A \vee B, D \vee \$, \$\rangle$$
$$= \langle 0.61, 0, 0, 0.15, 0.17, 0.04, 0.02\rangle$$

The corresponding evidential intervals are $A[0.61, 0.78]$, $B[0, 0.17]$, $C[0, 0]$, $D[0.15, 0.19]$, \$[0.02, 0.06]. Thus, the most likely fault is A, followed by D, which is the expected result based on the data above.

Rule-Based Calculation of Support Functions

There is motivation to put the previous procedure into a rule-based format to facilitate integration of the method into rule-based expert systems. We have found a method of expression of the above procedure as rules that can be programmed into existing expert system shells using simple manipulations of certainty factors.

Let us examine the possible sources of support for a proposition f when two knowledge sources are combined using Dempster's rule. For each constraint, f will appear in exactly one of the sets H^+, H^-, and H^0, in addition to appearing as an element of θ. Define H_i^f as the fault set in the ith constraint that contains f. It can be seen from Figure 4 that exactly four of the sixteen intersections between the two constraints will contain f. From Eq. 10, only the intersections containing f can contribute to $s(f)$, but not all of these intersections necessarily contribute to

	B 0.0	AvD 0.7	Cv$ 0.1	Θ 0.2
AvB 0.8	B 0.0	A 0.56	Φ 0.08	AvB 0.16
C 0.0	Φ 0.0	Φ 0.0	C 0.0	C 0.0
Dv$ 0.2	Φ 0.0	D 0.14	$ 0.02	Dv$ 0.04

Figure 3. Combination of BPMD's for example 5.

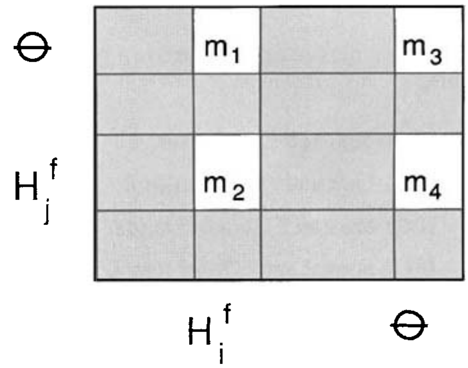

Figure 4. Intersections contributing support to f in combination of two BPMD's.

$s(f)$, since one or more of the intersections can be supersets of f. If we define $q(f)$ as the sum of the BPM's containing f in Figure 4, $q(f) = m_1 + m_2 + m_3 + m_4$, then $q(f)$ is an upper bound on the unnormalized value of $s(f)$.

The plausibility of f from Eq. 9 is one minus the sum of the BPM's of $\bar{}f$ and the subsets of $\bar{}f$. A set can be a subset of $\bar{}f$ if and only if it does not contain f. Therefore, at most twelve of the remaining intersections in Figure 4 can contribute support to $\bar{}f$. Less than twelve of these intersections will contribute to $s(\bar{}f)$ if mass is contributed to the empty set. Accordingly, an upper bound for the unnormalized value of $s(\bar{}f)$ is given by $1 - q(f)$. Since $p(f) = 1 - s(\bar{}f)$,

$$s(f) \le q(f) \le p(f). \quad (16)$$

Thus, $q(f)$ is guaranteed to lie in the evidential interval for f. It may also be seen that in the absence of uncertainty, $q(f) = s(f) = p(f)$, since under these conditions $s(f) = p(f)$. We refer to $q(f)$ as the supportability (support + plausibility) of hypothesis f.

Now let C_i^f be the condition of constraint i that corresponds to H_i^f, e.g., if f appears in H_i^+, then $C_i^f = C_i^+$. The C_i^f are simply the symptoms of the fault f, in terms of a pattern of violated and satisfied constraint. Let $CF(C_i^f)$, the certainty factor for C_i^f, be defined as the BPM assigned to the fault set H_i^f plus the uncertainty in the constraint:

$$CF(H_i^f) = BPM(H_i^f) + u_i \quad (17)$$

It can be seen from Figure 4 that $q(f)$ is simply the product of these certainty factors. For multiple knowledge sources, $q(f)$ is given by

$$q(f) = \Pi CF(H_i^f). \quad (18)$$

Therefore, the prototypical diagnostic rule can be written in the form:

$$\text{If } (C_1^f) \text{ and } (C_2^f) \text{ and} \ldots \text{then } (f), \quad (19)$$

where the premises are the complete pattern of constraint violations and satisfactions that result from the fault in question, and the supportability of f is the product of the certainty factors of the rule antecedents. This procedure results exactly in the unnormalized support functions of Shafer's theory, in the absence of uncertainty.

Example 6

The previous example can be expressed in a rule-based framework as follows:

If $C1$-high and $C2$-low then A

If $C1$-high and $C2$-high then B

If $C1$-low and $C2$-normal then C

If $C1$-normal and $C2$-low then D

If $C1$-normal and $C2$-normal then \$

With $b_1 = 0.8$, $b_2 = 0.7$, $\epsilon_1 > 0$, $\epsilon_2 < 0$, and $u_2 = 0.2$, the certainty factors for the rule antecedents are:

$$\mathrm{CF}(C1\text{-high}) = 0.8 \qquad \mathrm{CF}(C2\text{-high}) = 0.2$$
$$\mathrm{CF}(C1\text{-normal}) = 0.2 \qquad \mathrm{CF}(C2\text{-normal}) = 0.3$$
$$\mathrm{CF}(C1\text{-low}) = 0.0 \qquad \mathrm{CF}(C2\text{-low}) = 0.9$$

Taking the product of the antecedents in each rule, the supportability of each hypothesis is given by $q(A) = 0.72$, $q(B) = 0.16$, $q(C) = 0.0$, $q(D) = 0.18$, $q(\$) = 0.06$. These figures indeed lie between the support and the plausibilities calculated in example 5.

It is important to note that in the Boolean sense, the rule "If $C1$-low then C" is sufficient to diagnose the fault C, since C is the only fault capable of causing $C1$-low. However, because of uncertainty in the assertion "$C1$-low", the additional antecedent "and $C2$-normal" is necessary to accurately assess the possibility of fault C. Consider the case where $\mathrm{CF}(C1\text{-low}) = 0.5$. If $C2$ is very low, say $\mathrm{CF}(C2\text{-low}) = 0.9$, we would tend to reduce our belief in fault C, since we would prefer an explanation for $C2$-low (namely D). If $C2$ appears normal, this would tend to confirm our belief in fault C. Thus, even though fault C does not explicitly enter constraint 2, the condition of constraint 2 is important in formulating beliefs regarding the hypothesis C. This is why the uncertain reasoning considers all symptoms in rating faults, rather than just the minimum set required in a Boolean analysis.

Fuzzy Set Theory in the Rule-Based Format

We have now derived the syntax of rules implementing the method of governing equations, and a means for evaluating the supportability of a fault hypothesis. This process can be repeated using fuzzy set theory, yielding a somewhat different result.

Define a fuzzy set H_i as the set of faults supported by the evidence of the ith constraint. H_i may contain elements of H^+, H^-, and H^0, since partial support for each of these sets may be derived from a constraint simultaneously. Fuzzy set theory gives no insight on how membership grades are to be assigned to the members of this set; however, in light of the previous developments, a reasonable choice is to assign each fault a membership grade equal to the certainty factor of its parent set:

$$\chi_i(f) = \mathrm{CF}(H_i^f) \tag{20}$$

We have shown previously that in the Boolean case, the single-fault diagnosis is the intersection of the fault sets activated by the state of the constraints, Eq. 6. Similarly, the diagnosis under fuzzy set theory is the fuzzy intersection of the H_i, $i = 1, \dots NC$. The single-fault diagnosis, S_1, therefore contains not one element, but a set of possible faults, together with their respective membership grades.

Example 7

Using the same data as examples 5 and 6, the diagnosis is calculated as follows:

$$H_1 = \{(A, 0.8), (B, 0.8), (C, 0), (D, 0.2), (\$, 0.2)\}$$
$$H_2 = \{(A, 0.9), (B, 0.2), (C, 0.3), (D, 0.9), (\$, 0.3)\}$$
$$S_1 = H_1 \cap H_2 = \{(A, 0.8), (B, 0.2), (C, 0), (D, 0.2), (\$, 0.2)\}$$

From this example, it can be seen that the membership grade of fault f in S_1 is simply the minimum of the $\mathrm{CF}(H_i^f)$, $i = 1, \dots NC$. Thus, whereas the mathematical theory of evidence calculates the product of certainty factors, Eq. 18, fuzzy set theory takes the minimum of the certainty factors. The same rule format, Eq. 19, can be applied to both methods. This is easily confirmed by returning to example 6 and reproducing the result of example 7 by taking the minimum of the certainty factors in the rule antecedents instead of the product.

Interestingly, the minimum of the certainty of the rule antecedents also appears in confirmation theory (rule 1). Thus, in the context of rules written in the form of Eq. 19, fuzzy set theory and confirmation theory yield identical results.

Example Application

Figure 5 depicts a recycle reactor system consisting of a tubular reactor, pump, controllers, sensors, and associated piping. The operating fluid is assumed to be incompressible, and the flows are turbulent. Two proportional-integral controllers regulate the inlet flow rate and the recycle ratio. In this example, we ignore temperature and chemical effects and treat only flows and pressures. Nonetheless, this problem presents significant challenges due to material recycle, complex state feedback, and bidirectional transmission of pressure disturbances. We also subject each measurement to significant random noise. The model and numerical parameters defining this system are given in the Appendix.

Table 2 lists 26 faults affecting flows and pressures in this system, labeled A through Z. The faults involve blockages, leaks, and valve and controller malfunctions. Subtleties to note in Table 2 are:

1. Sensor failure to a fixed value (SENSOR-FAILS) and sensor bias (SENSOR-BIASED) are considered separately *in certain* cases. When the sensor is an input to a control loop, the set point of the loop will be maintained only under the latter condition, and thus the symptoms of the two faults are different. An exception is the case of F_3, where both a measurement bias and sensor failure will cause deviation from the set point. In cases where the symptoms of sensor failure and measurement bias are equivalent, a single fault (SENSOR-FAILS) is listed.

2. Controller and control valve failures are lumped together (CONTROLLER-FAILS). With the available measurements, it is impossible to distinguish controller faults from valve problems. This would not be the case if the controller output signal were used as an additional measurement.

3. Faults J and R (leaks) are subdivided as follows: J_1, leak

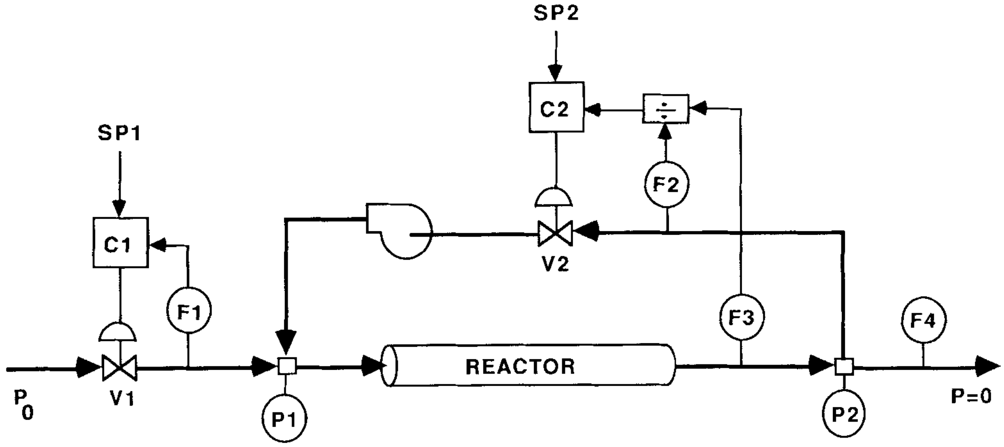

Figure 5. Flowsheet of recycle reactor.

between sensors P_1 and F_3; R_1, between P_2 and F_2; R_2, between F_3 and P_2; R_3, between P_2 and F_4. Note that $R \cap R_1 = R_1$, $R \cap {\sim}R_1 = \{R_2, R_3\}$, etc.

The governing equations for normal operation of the recycle reactor are shown in Table 3. The constraints involve the control objectives, mass balances, equations for fluid flow, and equations for the positions of the control valves. In these equations, all values are measured except the flow resistances, k_3 and k_4, which are nominally fixed. Note that the controller constraints have been written as (*variable*) − (*set point*) = 0, even though in fact this is not precisely true under normal operations.

Table 2. List of Faults for Recycle Reactor

A = C_1-FAILS-HIGH (controller or valve)
B = C_1-FAILS-LOW (controller or valve)
C = F_1-SENSOR-FAILS-HIGH
D = F_1-SENSOR-FAILS-LOW
E = F_1-SENSOR-BIASED-HIGH

F = F_1-SENSOR-BIASED-LOW
G = BLOCKAGE-INLET
H = P_1-SENSOR-FAILS-HIGH
I = P_1-SENSOR-FAILS-LOW
J = SUBSYSTEM-1-LEAK (between flowmeters 1, 2, 3)

K = F_2-SENSOR-FAILS-HIGH
L = F_2-SENSOR-FAILS-LOW
M = F_2-SENSOR-BIASED-HIGH
N = F_2-SENSOR-BIASED-LOW
O = BLOCKAGE-RECYCLE (or reduced pumping efficiency)

P = P_2-SENSOR-FAILS-HIGH
Q = P_2-SENSOR-FAILS-LOW
R = SUBSYSTEM-2-LEAK (between flowmeters 2, 3, 4)
S = C_2-FAILS-HIGH (controller or valve)
T = C_2-FAILS-LOW (controller or valve)

U = F_3-SENSOR-FAILS-HIGH
V = F_3-SENSOR-FAILS-LOW
W = BLOCKAGE-REACTOR

X = F_4-SENSOR-FAILS-HIGH
Y = F_4-SENSOR-FAILS-LOW
Z = BLOCKAGE-OUTLET

Additional conditions
$ = Normal operation
ϕ = No single fault explanation of symptoms

Numerical results indicate that this approximation is valid, and no spurious diagnoses are generated when set point changes are introduced with either non-Boolean technique. Table 3 also lists the faults on high and low violations of each of the six constraints on the recycle reactor. The faults listed with each constraint are sufficient conditions for violation of the constraint in the indicated direction, except those listed parenthetically, which cause constraint violation only when of sufficient magnitude to cause controller saturation. To reflect the uncertainty in symptom patterns for these faults, rules are modified to include both saturated and unsaturated behavior. For example, the rule for fault *C*1 is: If (*C*1–low or *C*1–normal) and *C*2–normal and (etc.). Otherwise, rules are derived from Table 3 in exactly the same way as the rules in example 6 were derived from Table 1.

The governing equations for more complex systems involving differential equations could be evaluated in either differential form by calculating rates of change of process measurements, or in integral form. The integral form would involve on-line simulation of the process equipment. Thus, for example, if the approximation of (*variable*) − (*set point*) = 0 is not sufficient for processes under large and frequent set point changes, a simulation of the expected process response can be substituted for the approximate controller constraint.

To demonstrate the Boolean approach, consider fault *W* (reactor blockage). For small blockages, all constraints are satisfied except the pressure drop relationship for the reactor (constraint 3), which is negative. Any one of the faults *H*, J_1, *Q*, *V*, or *W* would be sufficient to cause this violation. However, since the faults J_1, *Q*, and *V* would be sufficient to cause other

Table 3. Governing Equations and Fault Sets for Recycle Reactor

	Constraint	H^+	H^-
1	$F_1 - SP1 = 0$	D, B, (G, W, Z)	C, A
2	$F_2/F_3 - SP2 = 0$	L, T, (O, R_1, R_2)	K, S
3	$F_3 - k_3\sqrt{P_1 - P_2}$	H, J_1, Q, V, W	I, P, R_2, U
4	$F_4 - k_4\sqrt{P_2} = 0$	P, R_3, Y, Z	Q, X
5	$F_1 + F_2 - F_3 = 0$	D, F, L, N, U	C, E, J, K, M, V
6	$F_3 - F_2 - F_4 = 0$	K, M, V, X	L, N, R, U, Y

constraint violations, only faults H and W are possible. Evaluating through Eq. 6,

$$S_1 = {}^{\sim}\{D, B, C, A\} \cap {}^{\sim}\{L, T, K, S\} \cap \{H, J_1, Q, V, W\}$$
$$\cap {}^{\sim}\{P, R_3, Y, Z, Q, X\}$$
$$\cap {}^{\sim}\{D, F, L, N, U, C, E, J, K, M, V\}$$
$$\cap {}^{\sim}\{K, M, U, X, L, N, R, U, Y\}$$
$$= \{H, W\}$$

Thus, the method narrows the set of possibilities from 26 to two faults, and this is the limit of resolution for this particular fault. Unique diagnoses are rendered in the large majority of remaining cases.

In this example, faults O and G are not diagnosed unless they are of sufficient magnitude to cause controller saturation. In general, analysis of the intersections in Eq. 6 for each fault will indicate which faults cannot be detected, and which faults cannot be distinguished from each other with a given set of measurements and constraints. This information may be useful in selection and placement of sensors in process design or retrofit. Also, other methods (causal search, experiential knowledge) may be helpful in diagnosing faults that are not detectable or uniquely diagnosable by the method of governing equations (Kramer and Palowitch, 1985).

Table 4 shows the Boolean diagnosis as a function of time under normal operating conditions, using 90% confidence as the threshold for constraint violation. The diagnosis is subject to random fluctuations as thresholds are crossed due to measurement noise. These fluctuations can be reduced by increasing the size of the confidence interval or prefiltering, but only at the expense of reducing the sensitivity of the diagnosis. In Table 5, the Boolean diagnosis is shown for the case where inlet flow control valve is stuck at 70% open (fault A). Again, the diagnosis is subject to random fluctuations and records the correct diagnosis only sporadically.

Table 4. Boolean Diagnosis under Normal Operating Conditions

Time*	Diagnosis	Time	Diagnosis
1	$	68	φ
7	H	69	$
8	T	72	S
9	S	73	$
10	T	79	S
11	$	80	$
12	I	81	T
13	$	82	$
14	A	87	T
15	$	88	$
19	G	91	Z
20	φ	92	S
21	$	93	B
44	φ	94	$
45	$	96	T
50	A	97	$
51	$	99	Z
64	O	100	$
65	$		

*Time increment through next listed time

Table 5. Boolean Diagnosis for Valve 1 Stuck 70% Open

Time*	Diagnosis	Time	Diagnosis
101	$	133	φ
105	H	134	A
106	A	135	φ
109	$	136	A
110	W	141	$
111	φ	144	A
112	A	148	C
114	Z	149	A
115	A	150	$
116	X	152	φ
118	A	153	A
120	φ	156	X
121	A	157	A
124	φ	159	W
125	A	160	$
128	$	164	φ
131	φ	166	I
132	A		

*Time increment through next listed time

The diagnosis of the same fault by Shafer's method is shown in Figure 6. This plot shows the diagnosis at 100 time intervals before and after the introduction of the fault. The values $P(\chi_c^2) = 0.1$, $u_i = 0$, and $n = 4$ are used for assigning beliefs in this example. Qualitatively, the diagnosis is unchanged by moderate variations of these parameters. A continuous curve is obtained by passing the time series of $q(f)$ values through an exponential filter with a filtering parameter 0.9, and the resulting values are normalized so that the sum of all $q(f)$ equals one. This type of plot provides a clear visualization of the state of the process as a function of time. Under normal operation, the supportability $q(\$)$ ranges from 0.55 to 0.8, with all faults below the noise level (0.2). After the fault is introduced, $q(\$)$ falls to between 0.25 to 0.4, and $q(A)$ increases to the range 0.4 to 0.65, clearly indicating the presence of the fault. All other faults remain below the noise level.

The diagnosis generated through fuzzy set theory is depicted in Figure 7 for the same data. Quite surprisingly, the result is

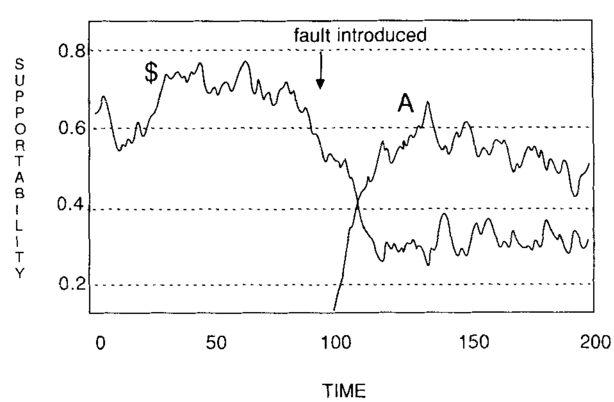

Figure 6. Diagnosis using mathematical theory of evidence.

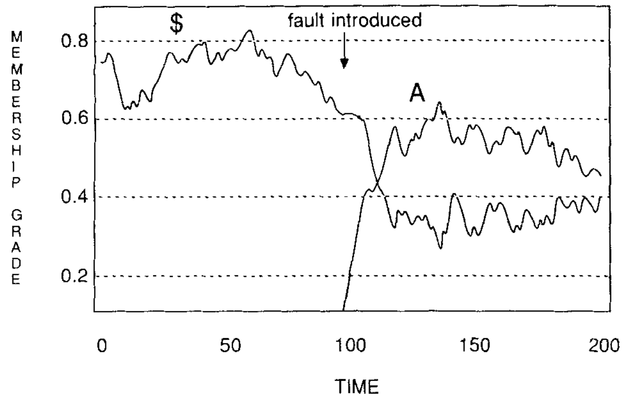

Figure 7. Diagnosis using fuzzy set theory.

virtually identical to the previous diagnosis, in spite of the fact that Shafer's method is based on the product of the CF's and the fuzzy set approach uses the minimum of the CF's. In all examples studied, the two methods perform equally well and provide strikingly similar results. We have no theoretical explanation for the similarity between the two methods.

Discussion

We have shown in this paper how expert systems can be applied to the diagnosis of faults in chemical processes using quantitative models of process performance. Numerical experiments run with these methods indicate that the methods are insensitive to the selection of belief function that describes the observed symptoms, and also are insensitive to the technique used to evaluate the supportability or certainty factor for the fault. This suggests that the MYCIN method of manipulating certainty factors, which has been proven in many expert systems, is adequate for implementing the method of governing equations as an expert system. The rule-based format allows the governing equations method to be integrated with experiential knowledge from process operators and engineers.

It should be stressed that even in a system without measurement noise, non-Boolean techniques are preferable to Boolean techniques because they provide a ranked list of fault possibilities. The Boolean set S_1 in Eq. 6 may be empty or it may exclude the correct fault, in which case no further information is available. When provided with a ranked list, if the operator is unable to verify the presence of the top-rated fault, then the second fault can be considered, and so on until the actual fault is found.

The probability of multiple or simultaneous faults, theoretically very small, may be of importance for several reasons:

1. Faults causing other faults (induced failures)
2. Latent faults that are not detectable until additional faults occur
3. Intentional operation in the presence of one or more faults, with the sudden occurrence of an additional fault

Diagnosis of simultaneous faults is a topic for future research.

We have not attempted to define the structural aspects of the expert system in this paper, other than at the level of the single rule. In building an expert system for a sizable plant, the structure of the knowledge base, defining which rules to apply and when, and methods of generating knowledge will be of great importance. Additionally, the human-factors engineering of these systems will be a key element in their effectiveness. These are problems for ongoing research.

Acknowledgment

The author gratefully acknowledges support of this research by the Shell Foundation, the Atlantic Richfield Foundation, and LISP Machine, Inc.

Notation

b_i = belief for ith constraint, Eq. 13
BPMD = basic probability mass distribution
CF = certainty factor, Eq. 17
C_i^+, C_i^-, C_i^0 = conditions of high and low constraint violation and constraint satisfaction, respectively, Eq. 1
C_i^* = actual condition of ith constraint
C_i^f = condition of ith constraint resulting from f
F = set of possible faults
F^* = set of actual faults
H_i^+, H_i^- = sets of faults sufficient to cause high and low violation of ith constraint, respectively, Eq. 2
H_i^0 = faults not sufficient to cause constraint violation, Eq. 4
H_i^* = fault set corresponding to C_i^*
h_{ij} = jth element of H_i^*
$\underline{H_i^*}$ = logical statement that at least one h_{ij} is true
$\overline{H_i^f}$ = fault set containing f in ith constraint
H_i = fuzzy set of faults supported by ith constraint
$m(A)$ = basic probability mass assigned to A
n = exponent, Eq. 13
NC = number of constraints
p = plausibility in Shafer's theory, Eqs. 9, 11
$P(\chi_i^2)$ = chi-squared probability distribution
q = supportability, Eq. 18
S_1 = set of viable single fault hypotheses
s = support in Shafer's theory, Eq. 10
u_i = uncertainty for ith constraint, Eq. 13
\$ = normal (fault-free) operation

Greek letters

ϵ_i = residual of ith constraint
σ_i = standard deviation of ϵ_i
$\chi_i^2 = (\epsilon_i/\sigma_i)^2$
χ = membership grade in a fuzzy set

Logic symbols

$\rightarrow$ = implication
$\leftrightarrow$ = logical equivalence
$\forall$ = universal quantifier
$\sim$ = negation
$\vee$ = disjunction (inclusive or)
$A\sim B$ = difference of sets (elements of A not in B)
$=$ = set equivalence
$\cup$ = union
$\cap$ = intersection
ϕ = empty set
$\wedge$ = conjunction (and)
$\in$ = element of
$\subset$ = subset

Appendix. Model and Parameters for Reactor Simulation

Controller parameters

Set point for $C1$, $SP1 = 1.0$
Set point for $C2$, $SP2 = 0.5$
Gain for $C1$ and $C2$, $g = 0.5$
Integral time for $C1$ and $C2$, $\tau = 2.0$
Nominal setting for $V1$ and $V2 = 0.5$ (50% open)
Simulation time increment = $\Delta t = 1$

Physical parameters

$k1$ = Flow coefficient for inlet stream = 1.0 * $V1$
$k2$ = Flow coefficient for recycle = 1.0 * $V2$
$k3$ = Flow coefficient for reactor = 1.0
$k4$ = Flow coefficient for exit stream = 1.0
Pump pressure difference, DP = 8.0 (assumed fixed)
Inlet pressure, PO = 9.0 (assumed fixed)
Outlet pressure = 0.0 (assumed fixed)
Standard deviation of noise in all measurements = 0.05

Model equations

$$F1 + F2 - F3 = 0$$
$$F3 - F2 - F4 = 0$$
$$F1 - k1 * V1\sqrt{P0 - P1} = 0$$
$$F2 - k2 * V2\sqrt{P2 + DP - P1} = 0$$
$$F3 - k3\sqrt{P1 - P2} = 0$$
$$F4 - k4\sqrt{P2} = 0$$
$$V1(t + \Delta t) = V1(t) + g^*[e1(t) - e1(t - \Delta t) + \Delta t^* e1(t)/\tau]$$
$$V2(t + \Delta t) = V2(t) + g^*[e2(t) - e2(t - \Delta t) + \Delta t^* e2(t)/\tau]$$
$$e1 = SP1 - F1$$
$$e2 = SP2 - F2/F3$$

Nominal steady state solution

$F1 = 1.0$
$F2 = 1.0$
$F3 = 1.0$
$F4 = 1.0$
$P1 = 5.0$
$P2 = 1.0$

Literature cited

Andow, P. K., "Real-Time Analysis of Process Plant Alarms Using a Minicomputer," *Comput. Chem. Eng.*, **4**, 143 (1980).
———, "Fault Diagnosis Using Intelligent Knowledge-Based Systems," *Chem. Eng. Res. Des.*, **63**, 368 (1985).
Andow, P. K., and F. P. Lees, "Process Computer Alarm Analysis: Outline of a Method Based on List Processing," *Trans. Inst. Chem. Eng.*, **53**, 195 (1975).
Beazley, W. G., "Prevention of Chemical Leaks Using Expert Systems," API Spring Meet., San Diego (1986).
Charniak, E., and D. McDermott, *Introduction to Artificial Intelligence*, Addison-Wesley, Reading, MA (1985).
Chester, D., D. Lamb, and P. Dhurjati, "Rule-Based Computer Alarm Analysis in Chemical Process Plants," *Proc. Micro-Delcon*, Newark, DE, 22 (1984).
Davis, J. F., W. F. Punch III, S. K. Shum, and B. Chandrasekaran, "Application of Knowledge-Based Systems for the Diagnosis of Operating Problems," Paper 70e, AIChE Nat. Meet., Chicago (1985).
Davis, R., "Diagnostic Reasoning Based on Structure and Behavior," *Artific. Intell.*, **24**, 347 (1984).
Fink, P. K., J. C. Lusth, and J. W. Duran, "A General Expert System Design for Diagnostic Problem Solving," *IEEE Trans. Pattern Anal. Machine Intell.*, **PAMI-7**, 553 (1985).
Garvey, T. D., J. D. Lawrence, and M. A. Fischler, "An Inference Technique for Integrating Knowledge from Disparate Sources," *Proc. 7th Int. Joint Conf. Artific. Intell.*, Vancouver, 319 (1981).
Genesereth, M. R., "The Use of Design Descriptions in Automated Diagnosis," *Artific. Intell.*, **24**, 411 (1984).
Hempel, C. G., "Studies in the Logic of Confirmation," *Aspects of Scientific Explanation and Other Essays in the Philosophy of Science*, Free Press, New York (1965).
Heuristics, Inc., Sacramento, CA, private communication (1985).
Iri, M., K. Aoki, E. O'Shima, and H. Matsuyama, "An Algorithm for Diagnosis of System Failures in the Chemical Process," *Comp. Chem. Eng.*, **3**, 489 (1979).
Isermann, R., "Process Fault Detection Based on Modeling and Estimation Methods—A Survey," *Automatica*, **20**, 387 (1984).
Kandel, A., *Fuzzy Techniques in Pattern Recognition*, Wiley, New York (1982).
Kramer, M. A., and B. L. Palowitch, Jr., "Expert System and Knowledge-Based Approaches to Process Malfunction Diagnosis," Paper 70b, AIChE Nat. Meet., Chicago (1985).
Kumamoto, H., K. Ikenchi, K. Inoue, and E. J. Henley, "Application of Expert System Techniques to Fault Diagnosis," *Chem. Eng. J.*, **29**, 1 (1984).
Lamb, D., D. L. Chester, and P. Dhurjati, "An Academic/Industry Project to Develop an Expert System for Chemical Process Fault Detection," Paper 70c, AIChE Nat. Meet., Chicago (1985).
Lees, F. P., "Process Computer Alarm and Disturbance Analysis: Review of the State of the Art," *Comput. Chem. Eng.*, **7**, 669 (1983).
Mah, R. S. H., G. M. Stanley, and D. M. Downing, "Reconciliation and Rectification of Process Flow and Inventory Data," *Ind. Eng. Chem. Process Des. Dev.*, **15**, 175 (1976).
Mah, R. S. H., and A. C. Tamhane, "Detection of Gross Errors in Process Data," *AIChE J.*, **28**, 828 (1982).
Madron F., "A New Approach to the Identification of Gross Errors in Chemical Engineering Measurements," *Chem. Eng. Sci.*, **40**, 1855 (1985).
Martin-Solis, G. A., P. K. Andow, and F. P. Lees, "Fault Tree Synthesis for Design and Real-Time Applications," *Trans. Inst. Chem. Eng.*, **60**, 14 (1982).
Moore, R. L., private communication (1985).
Moore, R. L., L. B. Hawkinson, M. E. Levin, and C. G. Knickerbocker, "Expert Control," *Proc. ACC*, Boston, 885 (1985).
Moore, R. L., and M. A. Kramer, "Expert Systems in On-Line Process Control," *Chem. Proc. Control III*, Asilomar, CA (1986).
Patil, R. S., P. Szolovits, and W. B. Schwartz, "Causal Understanding of Patient Illness in Medical Diagnosis," *Proc. 7th Int. Joint Conf. Artific. Intell.*, Vancouver (1981).
Pople, H., "Heuristic Methods for Imposing Structure on Ill-Structured Problems: The Structuring of Medical Diagnostics," *Artificial Intelligence in Medicine*, P. Szolovits, ed., Westview, Boulder, CO (1982).
Romagnoli, J. A., and G. Stephanopoulos, "On the Rectification of Measurement Errors for Complex Chemical Plants," *Chem. Eng. Sci.*, **35**, 1067 (1980).
———, "Rectification of Process Measurement Data in the Presence of Gross Errors," *Chem. Eng. Sci.*, **36**, 1849 (1981).
Shafer, G., *A Mathematical Theory of Evidence*, Princeton Univ. Press, (1976).
Shiozaki, J., H. Matsuyama, E. O'Shima, and M. Iri, "An Improved Algorithm for Diagnosis of System Failures in the Chemical Process," *Comp. Chem. Eng.*, **9**, 285 (1985).
Shortliffe, E. H., *Computer-Based Medical Consultations: MYCIN*, American Elsevier/North Holland, New York (1976).
Shortliffe, E. H., and B. G. Buchanan, "A Model of Inexact Reasoning in Medicine," *Math. Biosci.*, **23**, 351 (1975).
Stanley, G. M., and R. S. H. Mah, "Estimation of Flows and Temperatures in Process Networks," *AIChE J.*, **23**, 642 (1977).
Tsuge, Y., J. Shiozaki, H. Matsuyama, and E. O'Shima, "Fault Diagnosis Algorithms Based on the Signed Digraph and Its Modifications," *I. Chem. Eng. Symp. Ser.*, **92**, 133 (1985).
Ungar, L. F., "A Framework for Fault Analysis," Paper 70d, AIChE Nat. Meet., Chicago (1985).
Watanabe, K., and D. M. Himmelblau, "Fault Diagnosis in Nonlinear Chemical Processes. I: Theory," *AIChE J.*, **29**, 243 (1983a).
———, "Fault Diagnosis in Nonlinear Chemical Processes. II: Application to a Chemical Reactor," *AIChE J.*, **29**, 250 (1983b).
———, "Incipient Fault Diagnosis of Nonlinear Processes with Multiple Causes of Faults," *Chem. Eng. Sci.*, **39**, 491 (1984).
Yoon, E. S., "Process Failure Diagnosis Using the Symptom Sub-Tree Model," Ph.D. Thesis, Massachusetts Inst. Tech. (1982).
Zadeh, L. A., "Fuzzy Sets," *Inf. Control*, **8**, 338 (1965).

Manuscript received Feb. 26, 1986, and revision received May 9, 1986.