ISE

ISE-TR-90-81

A MATHEMATICAL ANALYSIS OF INTERDEPENDENCE BETWEEN SAFETY CONTROL POLICY AND MULTI-SENSOR FUSION SCHEME VIA DEMPSTER-SHAFER THEORY

by

Toshiyuki Inagaki

May 1,1990

INSTITUTE
OF
INFORMATION SCIENCES AND ELECTRONICS
UNIVERSITY OF TSUKUBA

A Mathematical Analysis of Interdependence between Safety Control Policy and Multi-Sensor Fusion Scheme via Dempster-Shafer Theory

Toshiyuki Inagaki

Institute of Information Sciences and Electronics
University of Tsukuba
Tsukuba 305 Japan

Summary & Conclusions -- The Dempster-Shafer (DS) theory has been attaining its popularity in various fields in which some ignorance exists in our knowledge about an object. The DS theory may find some applications in system reliability and safety area. This paper shows that inadvertent application of the DS theory to safety control problems can degrade plant safety. We prove this in two phases: The first phase gives a new and unified rule of combination for fusing information on plant state which are given by independent knowledge sources such as sensors or human operators. The second phase proves that we cannot choose a rule of combination in an arbitrary manner among possible alternatives; viz, we must make a right choice of a combination rule depending on whether our safety control policy is of 'fault-warning type' or of 'safety-presentation type'. The optimal rule of combination for fault-warning type policies differs from that for safety-presentation type policies and there exists no single rule of combination which is optimal for both types of safety control policies at the same time.

1. INTRODUCTION

In dealing with large complex plants such as nuclear reactors, spacecrafts, it may not be wise to say that our knowledge about these plants is complete and perfect. We may be able to judge easily whether a plant is in its normal and safe operating conditions or in its abnormal and unsafe operating conditions. We often encounter situations, however, in which we does not have enough amount of evidence to conclude definitely whether the plant is safe or not. In these situations we may say, for example, "we are 60% sure that our plant is safe", where a proposition "our plant is safe" is supplied with the 'degree of belief' 0.6 concerning the truth of the proposition.

If we define the degree of belief for a proposition as the probability that the proposition is true, the degree of belief does not necessarily represent our exact intention that we have in mind. Consider a case in which we can distinguish two states for a plant; safe or unsafe. Suppose we make a statement, based on some available evidence and our knowledge, "our plant is safe with probability 0.6". Then we are forced to make another statement "our plant is not safe with probability 0.4", even though we have actually no intention to express our degree of belief concerning the truth of the proposition that our plant is unsafe. The latter statement is a consequence of the axiom of additivity in probability theory.

We assigned, in the above situation, the degree of belief 0.6 to the proposition "our plant is safe" just because we lack some evidence which convinces us of plant safety. In other words, the remaining 0.4 represents the degree that we are reluctant to say neither that the plant is safe nor that the plant is unsafe, because of our 'ignorance' concerning the current and true operating condition of the plant. The followings are two extreme cases which are permissible in this situation. (1) If we should be provided with, at some later time point, some evidence which supports unsafety of the plant, then the whole amount of 0.4 would be the degree of belief in unsafety of the plant. (2) If we should find finally some missing evidence which supports plant safety, then 0.4 would be added to 0.6 so that our degree of belief in plant safety would become unity.

The Dempster-Shafer (DS) theory [1] has been developed to give a reasonable tool for representing situations in which some various kinds of ignorance exist in our knowledge or information about an object; eg, the current operating condition of the plant, in the above example. A measure called a 'basic probability assignment' is defined on the finite set of propositions under a set of axioms. The set of axioms is looser than that for usual probability measure (for instance, additivity is not assumed for the basic probability assignment). It can be said that the basic probability assignment is a generalized version of probability measure defined on a sample space consisting of a finite number of sample points; a basic probability assignment can be constructed so that it coincides with an arbitrarily given probability measure. (It should not be understood, however, that the probability theory is a proper subset of the DS theory. The basic probability assignment can not replace the probability measure defined on a sample space consisting of a countably or uncountably infinite number of sample points, at least at the present time.)

The DS theory has been attaining its popularity in various fields including artificial intelligence [2], medical diagnosis [3], target identification [4]. It would be possible for the DS theory to find some applications in the area of system reliability and safety. However careful investigation must be exercised; inadvertent application of the DS theory can degrade plant safety. We will prove this mathematically by taking, as an example, a safety control problem in which we must decide whether to operate or shutdown a plant based on possibly imperfect information given by independent 'knowledge sources', where knowledge sources include conventional sensors, intelligent sensors, human operators, and their combinations. The crucial point lies in a 'rule of combination' which is an algorithm to fuse or combine several sets of information given by independent knowledge sources. Two rules of combinations are known currently in the most basic settings: Dempster's rule [1] and Yager's rule [5]. Dempster's rule of combination is the oldest one and is commonly used in various applications, eg [2-4]. It is shown recently that Demspter's rule gives counterintuitive results and exhibits numerical instability in some cases which are not uncommon [6, 7]. Yager's rule has been proposed as an alternative rule of combination which is free from these disadvantages of Dempster's rule.

This paper analyzes in two phases the applicability of the DS theory to safety control problems where a set of information on plant state is given by independent knowledge sources. The first phase of our present paper gives a new and unified rule of combination which includes Dempster's rule and Yager's rule as its special cases. With the unified rule of combination we will show in the second phase of the paper that we cannot choose a rule of combination in an arbitrary manner among the whole set of combination rules if our aim lies in maintaining plant safety. The following two types of policies are distinguished for safety control of plants: (1) a safety control policy of 'fault-warning type', and (2) a safety control policy of 'safety-presentation type'. This distinction has some parallels with classifications of human-machine interface configurations given in [8]. We define a safety control policy of fault-warning type as one which shuts down a plant only when the plant is judged as being unsafe. A typical example of the fault-warning type policy can be found at the launch of the space shuttle Challenger in January of 1986. An engineer advised not to launch Challenger because he could not be sure of safety of Challenger in the severe weather condition. That did not mean that Challenger was actually proven to be unsafe, and thus Challenger was launched. A safety control policy of safety-presentation type is defined as one which allows a plant to operate only when the plant is judged as being safe. If we had taken this type of policy, Challenger would not have been launched. We will prove mathematically that we must use the right rule of combination in the right place; viz, there exists no single rule of combination which is optimal for both types of safety control policy.

Notation

X frame of discernment which consists of a finite number of propositions

2^X power set of X; viz, the family of sets consisting of all the subsets of X

m basic probability assignment function

m_i basic probability assignment specified by the i-th knowledge source

q ground probability assignment function; viz,

$$q(C) = \sum_{A \cap B = C} m_1(A)\, m_2(B), \qquad A \subset X,\ B \subset X$$

$\emptyset$ null set, or a proposition which is always false

2. Rules of Combination in Dempster-Shafer Theory

2.1. Preliminaries

A basic probability assignment function $m : 2^X \rightarrow [0, 1]$ satisfies the following set of axioms:

I. $m(A) \geq 0$ for any $A \in 2^X$ (1)

II. $m(\emptyset) = 0$ (2)

$$\text{III. } \sum_{A \subset X} m(A) = 1 \tag{3}$$

Suppose we have two sets of basic probability assignments $\{m_1(A): A \subset X\}$ and $\{m_2(B): B \subset X\}$ which are given by the independent knowledge sources and suppose we want to fuse them into a single basic probability assignment. A straightforward way of combination may be to compute

$$q(C) = \sum_{A \cap B = C} m_1(A)\, m_2(B) \tag{4}$$

The ground probability assignments $\{q(C): C \subset X\}$, however, cannot necessarily be a basic probability assignment because $q(\emptyset) \geq 0$, in general. We thus need a 'rule of combination' for transforming the ground probability assignment into the basic probability assignment .

The following rules of combination are known in the most basic settings:

(A) Dempster's rule [1]:

$$m(C) = q(C) / \{1 - q(\emptyset)\} \tag{5}$$

(B) Yager's rule [5]:

$$m(C) = q(C)\,, \quad C \neq \emptyset, X \tag{6a}$$

$$m(X) = q(X) + q(\emptyset) \tag{6b}$$

Dempster's rule has a distinctive feature in neglecting every contradiction which may be found among information from independent knowledge sources, which is a consequence of normalization of the ground probability assignment q; see, (5). Because of the normalization, Dempster's rule can give counterintuitive results and can exhibit numerical instability in some cases [6, 7]. Yager's rule regards, on the other hand, any contradiction among information from independent knowledge sources as our ignorance; see, (6b). Yager's rule may seem to be more careful and modest than Dempster's rule. However this is not always true, which we will prove in §3.1.

2.2 Unified Rule of Combination

Any rule of combination can be expressed as:

$$m(C) = q(C) + f(C)\, q(\emptyset)\,, \quad C \neq \emptyset \tag{7a}$$

$$\sum_{C \subset X,\, C \neq \emptyset} f(C) = 1\,, \quad f(C) \geq 0 \tag{7b}$$

Consider a class of combination rules for which the following property holds:

$$m(C) / m(D) \;=\; q(C) / q(D) \tag{8}$$

for any C and D which are distinct from X or Ø. Eq. (8) implies that we have no knowledge on relative importance or credibility between propositions C and D. A necessary and sufficient condition for (8) to hold is:

$$f(C) / q(C) \;=\; k \quad \text{for any } C \neq X, \emptyset \tag{9}$$

A unified rule of combination is then given as follows:

$$m(C) = \{1 + k\, q(\emptyset)\}\, q(C)\,, \quad C \neq X, \emptyset \tag{10a}$$

$$m(X) = \{1 + k\, q(\emptyset)\}\, q(X) + \{1 + k\, q(\emptyset) - k\}\, q(\emptyset) \tag{10b}$$

$$0 \leq k \leq \;\{1 - q(\emptyset) - q(X)\}^{-1} \tag{10c}$$

The unified rule of combination (10) coincides with Yager's rule when $k = 0$ and coincides with Dempster's rule when $k = \{1 - q(\emptyset))\}^{-1}$. Note that:

$$\{1 - q(\emptyset)\}^{-1} \;\leq\; \{1 - q(\emptyset) - q(X)\}^{-1}\,, \tag{11}$$

which shows the existence of rules of combination which 'extrapolate' rules of Yager and Dempster (see, Fig. 1).

3. Rule of Combination and Safety Control Policy

Let S denote the proposition "the plant is safe" and U denote the proposition "the plant is unsafe". Consider the case in which the frame of discernment X consists of the above two propositions; X = {S, U}. Then the proposition "we cannot judge whether the plant is safe or not" is represented as X itself.

Suppose we have received two sets of basic probability assignments $\{m_i(S), m_i(U), m_i(X)\}$, $(i = 1, 2)$ from a couple of independent knowledge sources. They are combined by (10) into a single basic probability assignment $\{m(S), m(U), m(X)\}$ (see, Fig.2):

$$m(S) = \{1 + k\, q(\emptyset)\}\, q(S) \tag{12}$$

$$m(U) = \{1 + k\, q(\emptyset)\}\, q(U) \tag{13}$$

$$m(X) = \{1 + k\, q(\emptyset)\}\, q(X) + \{1 + k\, q(\emptyset) - k\}\, q(\emptyset) \tag{14}$$

3.1 Control Policy of Fault-Warning Type

Let GO denote our decision to put the plant into operation or not to shutdown the plant which is currently working. Let SD denote our decision to shutdown the plant or not to allow the plant to start its operation. A safety control policy of fault-warning (FW) type is defined by the following map FW from the set of propositions $\{S, U, X\}$ to the set of decisions $\{GO, SD\}$:

$$FW : \{S, X\} \rightarrow \{GO\}, \quad FW : \{U\} \rightarrow \{SD\} \tag{15}$$

Let m(GO:FW) and m(SD:FW) denote basic probability assignments for decisions GO and SD, respectively, under a fault-warning type control policy. We have:

$$m(GO{:}FW) = m(S) + m(X)$$

$$= \{1 + k\, q(\emptyset)\}\{q(S) + q(X)\} + \{1 + k\, q(\emptyset) - k\}\, q(\emptyset) \tag{16a}$$

$$m(SD{:}FW) = m(U)$$

$$= \{1 + k\, q(\emptyset)\}\, q(U) \tag{16b}$$

Note that m(GO:FW) is monotone non-increasing with k. Consider the following three specific rules of combination: (a) Yager's rule, which is obtained if we set $k = 0$ in (10), (b) Dempster's rule, where $k = \{1 - q(\emptyset)\}^{-1}$, (c) the extreme rule among combination rules of extrapolation type, where we set $k = \{1 - q(\emptyset) - q(X)\}^{-1}$. Then we have:

$$m(GO{:}FW{:}Yager) \geq m(GO{:}FW{:}Dempster) \geq m(GO{:}FW{:}Extrapolation) \tag{18}$$

We have, in a similar manner, the following order relation on m(SD:FW):

$$m(SD{:}FW{:}Yager) \leq m(SD{:}FW{:}Dempster) \leq m(SD{:}FW{:}Extrapolation) \quad (19)$$

These order relations show that, among all combination rules represented by (10), Yager's rule has the largest possibility of failing to shutdown the unsafe plant. The rule of combination with $k = \{1 - q(\emptyset) - q(X)\}^{-1}$, which has not been known before the unified rule of combination (10) is given, is optimal for maintaining plant safety under safety control policy of fault-warning type.

3.2 Control Policy of Safety-Presentation Type

A control policy of safety-presentation (SP) type is defined by the following map SP:

$$SP : \{S\} \rightarrow \{GO\}, \quad SP : \{U, X\} \rightarrow \{SD\} \quad (20)$$

We have the basic probability assignments m(GO:SP) and m(SD:SP) for decisions GO and SD, respectively, as follows under a safety-presentation (SP) type control policy :

$$\begin{aligned} m(GO{:}SP) &= m(S) \\ &= \{1 + k\, q(\emptyset)\}\, q(S) \quad (21) \\ m(SD{:}SP) &= m(U) + m(X) \\ &= \{1 + k\, q(\emptyset)\}\, \{q(U) + q(X)\} + \{1 + k\, q(\emptyset) - k\}\, q(\emptyset) \quad (22) \end{aligned}$$

Note that m(GO:SP) is monotone non-decreasing with k. Thus we have the following order relation for the three specific rules of combination discussed in §3.1:

$$m(GO{:}SP{:}Yager) \leq m(GO{:}SP{:}Dempster) \leq m(GO{:}SP{:}Extrapolation) \quad (23)$$

Similarly we have:

$$m(SD{:}SP{:}Yager) \geq m(SD{:}SP{:}Dempster) \geq m(SD{:}SP{:}Extrapolation) \quad (24)$$

The above order relations show that, among all possible rules of combination represented by eq. (10), Yager's rule is optimal for maintaining plant safety under control policy of safety-presentation type.

4. Topics for Further Research

It would be preferable if we could avoid unnecessary plant shutdowns. Under a control policy of fault-warning type, we can lessen possibility of unnecessary plant shutdowns by assigning a lesser value to k in (10) in exchange for more possibility of failing to shutdown the unsafe plant. Under a control policy of safety-presentation type, on the other hand, we can lessen unnecessary plant shutdowns by assigning a larger value to k in (10) in exchange for more possibility of accidents. One of the further research topics would be to analyze how we can determine an optimal rule of combination or an optimal value of k in each type of control policy.

The second topic is on the ordering of information fusion if we have more than two sets of basic probability assignments concerning plant state. Let $m_1 \oplus m_2$ denote a basic probability assignment function which is obtained by combining two sets of basic probability assignments m_1 and m_2. A rule of combination is said to be associative if:

$$((m_1 \oplus m_2) \oplus m_3)(A) = (m_1 \oplus (m_2 \oplus m_3))(A) \quad \text{for any } A \subset X \qquad (25)$$

It is easy to show that the unified rule of combination (10) is associative if and only if k $= \{1 - q(\emptyset)\}^{-1}$, where (10) coincides with Dempster's rule. If an optimal rule of combination, which is determined by solving some optimization problem, should be distinct from Dempster's rule, $((m_1 \oplus m_2) \oplus m_3)(A) \neq (m_1 \oplus (m_2 \oplus m_3))(A)$ for some $A \subset X$. Thus we must analyze the effect of non-associativity of the optimal rule of combination on our decision of safety control.

ACKNOWLEDGMENT

This research was supported by The Ministry of Education, Science and Culture under Grant-in-Aid for Scientific Research 01550320.

REFERENCES

[1] G. Shafer, *A Mathematical Theory of Evidence*, Princeton University Press, 1976.

[2] P.R. Cohen, *Heuristic Reasoning about Uncertainty: An Artificial Intelligence Approach*, Pitman, 1985.

[3] J. Gordon, E.H. Shortliffe, "The Dempster-Shafer theory of evidence and its relevance to expert systems", In B.G. Buchanan, E.H. Shortliffe (Eds.), *Rule-Based Expert Systems -- The MYCIN Experiments of the Stanford Heuristic Programming Project*, Chapter 13, Addison-Wesley, 1984.

[4] P.L. Bogler, "Shafer-Dempster reasoning with applications to multisensor target identification systems", *IEEE Trans. Syst., Man, Cybern.*, vol SMC-17, no 6, pp 968-977, 1987.

[5] R.R. Yager, "On the Dempster-Shafer framework and new combination rules", *Information Sciences*, vol 41, pp 93-137, 1987.

[6] L.A. Zadeh, "Review of Shafer's *A Mathematical Theory of Evidence*", *AI Magazine*, vol 5, no 3, pp 81-83, 1984.

[7] D. Dubois, H. Prade, "Combination and propagation of uncertainty with belief functions", *Proc. Ninth International Joint Conference on Artificial Intelligence*, vol 1, pp 111-113, 1985.

[8] T. Inagaki, Y. Ikebe, "A mathematical analysis of human-machine interface configurations for a safety monitoring system", *IEEE Trans. Reliability*, vol R-37, no 1, pp 35-40, 1988.

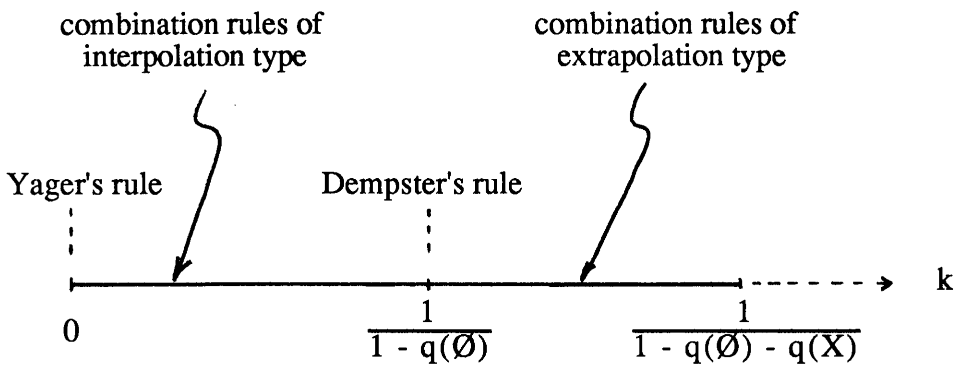
combination rules of interpolation type
combination rules of extrapolation type
Yager's rule
Dempster's rule
k
0
$\frac{1}{1 - q(\emptyset)}$
$\frac{1}{1 - q(\emptyset) - q(X)}$

Fig.1 Whole set of combination rules represented by the unified expression (10) with parameter k

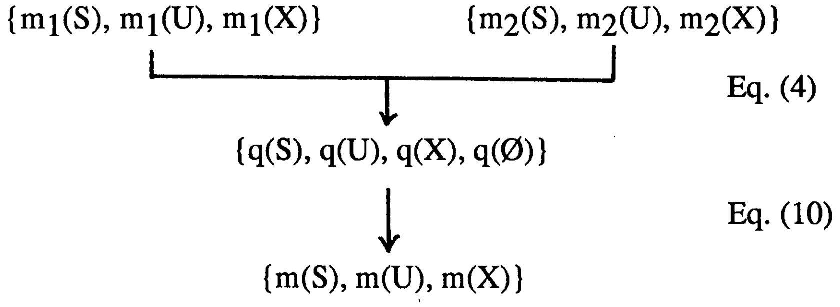
$\{m_1(S), m_1(U), m_1(X)\}$
$\{m_2(S), m_2(U), m_2(X)\}$
Eq. (4)
$\{q(S), q(U), q(X), q(\emptyset)\}$
Eq. (10)
$\{m(S), m(U), m(X)\}$

Fig.2 Process of combining two belief structures

INSTITUTE OF INFORMATION SCIENCES AND ELECTRONICS
UNIVERSITY OF TSUKUBA
TSUKUBA-SHI, IBARAKI 305 JAPAN

REPORT DOCUMENTATION PAGE	REPORT NUMBER ISE-TR-90-81

TITLE

A Mathematical Analysis of Interdependence between Safety Control Policy and Multi-Sensor Fusion Scheme via Dempster-Shafer Theory

AUTHOR(S)

Toshiyuki Inagaki; Institute of Information Sciences and Electronics;
University of Tsukuba; Tsukuba 305 JAPAN.

REPORT DATE May 1, 1990	NUMBER OF PAGES 12
MAIN CATEGORY Reliability theory	CR CATEGORIES

KEY WORDS

Multiple sensor fusion, Safety control, Fault-warning and safety-presentation, Dempster-Shafer theory, Rules of combination

ABSTRACT

Summary & Conclusions -- The Dempster-Shafer (DS) theory has been attaining its popularity in various fields in which some ignorance exists in our knowledge about an object. The DS theory may find some applications in system reliability and safety area. This paper shows that inadvertent application of the DS theory to safety control problems can degrade plant safety. We prove this in two phases: The first phase gives a new and unified rule of combination for fusing information on plant state which are given by independent knowledge sources such as sensors or human operators. The second phase proves that we cannot choose a rule of combination in an arbitrary manner among possible alternatives; viz, we must make a right choice of a combination rule depending on whether our safety control policy is of 'fault-warning type' or of 'safety-presentation type'. The optimal rule of combination for fault-warning type policies differs from that for safety-presentation type policies and there exists no single rule of combination which is optimal for both types of safety control policies at the same time.

SUPPLEMENTARY NOTES