IN THE NAME OF ALLAH,

THE MOST MERCIFUL,

THE MOST GRACIOUS

JKAU: Comp. IT. Sci., Vol. **3,** 128 Pages (2014 A.D. / 1436 A.H.) ISSN: 1658-6336
Legal Deposit 1435/1028

Journal of

KING ABDULAZIZ UNIVERSITY

Computing and Information Technology Sciences

Volume 3

2014 A.D. / 1436 A.H.

Scientific Publishing Centre
King Abdulaziz University
P.O. Box 80200, Jeddah 21589
Saudi Arabia
http://spc.kau.edu.sa

Copy Price

- Local : SR 10.00
- External : US$ 10.00

Subscription

Scientific Publishing Centre, King Abdulaziz University
P.O. Box 80200, Jeddah 21589, Saudi Arabia

Exchange

Deanship of Library Affairs, King Abdulaziz University
P.O. Box 80213, Jeddah 21589, Saudi Arabia

(English Section)

(Arabic Section)

(English Section)

JKAU: Comp. IT., **Vol. 3**, pp: 3 - 49 (2014 A.D./ 1436 A.H.)

DOI: 10.4197 / Comp. 3 -1.1

A Use-Modify Framework to Detect Feature Interactions in Web Services

Ahmed Khoumsi and **Zohair Chentouf***

*Department of Elect. & Comp. Eng., University of Sherbrooke, Sherbrooke, Canada, and *Software Engineering Department, College of Information and Computer Sciences, King Saud University, Riyadh, KSA*

zchentouf@ksu.edu.sa

Abstract. Composing Web services is often beneficial since created the new Web services from existing ones. However, Web service composition is prone to feature interactions, which denote undesirable behaviors arising when several Web services are used together. The existing methods for detecting feature interactions suffer generally from state space explosion. In this paper, we develop a method to detect feature interactions in Web services, which targets the reduction of state space explosion while trying to keep an acceptable power of feature interaction detection. The proposed method is based on the use of a language called Use-Modify which models Web services at a high abstraction level. A Use-Modify model of a Web service provides information such as “who uses what”, “who modifies what”, and characterizes each operation of use and modifying by “always”, “sometimes”, “never” and “maybe”. "Use-Modify" also indicates, for each use and modifies, whether there are conditions which may specified or unspecified. We study the computational complexity of our feature interaction detection method and demonstrate its applicability in several examples.

Keywords: Composing web services; Feature interaction detection; High abstraction level; Use-Modify relation; Use-Modify model.

1. Introduction

When existing Web Services (WS) are *composed* to create new WSs, the latter can contain undesired behaviors, which are called *feature interactions* (FI). Here is an example of FI in WS: we consider a supplier to which orders can be sent. When his stock is empty, a supplier forwards any incoming order to another supplier. Consider two WSs *Supplier*$_1$ and *Supplier*$_2$, an assuming that an order is sent to *Supplier*$_1$ and those both *Suppliers* have their stocks empty. We may have a following situation: *Supplier*$_1$ forwards an order to *Supplier*$_2$ which in turn the forwarding of the order to *Supplier*$_1$. The FI manifests itself by a blocking situation where each supplier is waiting the answer of the other.

FIs have been intensively studied in telecommunication services (or Telecom-services)[1-9], and ever since more recently in WSs. Many methods have been developed to detect FIs, some of them are rigorous and have a high power of FI detection. But the latter suffer from state space of explosion, such as those applying model-checking techniques. The approach we are proposing to detect FIs in WSs targets, the reduction of such a state space explosion problem while trying to keep an acceptable power of FI detection. We model the behaviors of WSs by so-called Use-Modify language (or UM-language) which is a high abstraction level formalism whose basic principle is to specify "who uses what" and "who modifies what". UM-language permits also to characterize each "use" and "modify" by "always", "sometimes", "never" or "maybe". Moreover, UM-language may also indicate conditions to "use" or "modify".

Our Use-Modify approach is slightly inspired by many workers[10,11]. Our contribution is that while[10-11] are mainly based on intuitive ideas, we adopt a much more rigorous approach where all our ideas are studied thoroughly and formally. A much shorter version of our paper is published in 2012[12].

The structure of the paper and its contributions compared to Khoumsi, *et al*.,[12] are as follows:

- In Section 2, we explain some fundamental differences between composing WSs and composing Telecom-services.
- Section 3 presents some related work on modeling and composing WSs and detecting their FIs.
- In Section 4, we propose a Use-Modify language (or UM-language) to model WSs at a high abstraction level. A UM-model is a set of UM-relations like "L uses R" or "L modifies R", where L and R represent WSs, functionalities of WSs or variables of WSs, and each "use" and "modify" is characterized by "always", "sometimes", "never" or "maybe". Here are specific contributions in comparison with those of Khoumsi, *et al*.,[12].

- the semantics of "use" and "modify" and their characterizations are defined more clearly and rigorously (Sect. 4.2);
- The identified Formal conditions to characterize UM-relations as well-formed (Sect. 4.3);
- Formal conditions can be associated with UM-relations to restrict their general semantics (Sect. 4.5).
- Section 5 proposes a number of logical rules that permit to enrich a UM-model in function of deriving new UM-relations from given UM-relations. Here are specific contributions in comparison with[12]:
- We first define fundamental rules which do not refer to UM-relations (Section 5.1); they are rather based on general logical statements; these rules are absent in Khoumsi, *et al.*,[12].
- Three categories of UM-rules (*i.e.* applicable rules of UM-relations) are deduced from the fundamental rules. (Section 5.2-5.4), instead of being partially defined without justification and categorization (as in Khoumsi, *et al.*,[12]).
- Soundness and completeness of the fundamental rules and the UM-rules are rigorously studied and discussed (Sections 5.5-5.6).
- Utility of characterizing "use" and "modify" by "maybe" is explained (Section 5.6.3).
- In Section 6, we are going to present a Use-Modify-based & method of detecting FIs in WSs. Contrary to that of Khoumsi, *et al.*,[12]:
- The method is specified as: Three-steps first algorithm where we indicate clearly what is done automatically and what is done by the designer.
- Second (which is not an easily understandable[12]) is illustrated by an abstract example throughout Sect. 6.2.
- We study the computational complexity of our FI detection method.
- Section 7 to demonstrates the applicability of our method for detecting all of the FIs of the benchmark[13] is a part of the FI[14].
- In Section 8, we demonstrate that our method can be used to detect several FIs, and we never only consider the WS composition, but also a Telecom-service composition and a mixed composition of WS including to the Telecom-service[15].

- Section 9 conclusions and by recapitulating of the contributions and proposing are some of the future work.
- Section 10 contains the proofs of some propositions; where Khoumsi, *et al*.,[12] not all of the propositions.

2. Web Service Composition Versus Telecommunication Service Composition

Let us show that composing WSs is different from composing Telecom-services.

1. Telecom-services can generally be abstracted by a few parameters. For example[16], each service is abstracted by a triggering party, and origin and destination parties. The services[17], are abstracted by some processing points that correspond to the main steps in a phone call. On the other hand contrary, WSs cannot be so simply abstracted, because a WS can be provided any imaginable software system providing a service through the Web.
2. Composing two Telecom-services generally means running them in parallel. Most of the FI studies for Telecom-services are based on this simple composition approach. On the contrary, WS composition means designing a new WS by composing existing WSs, based on the principle of software reusability. Hence, WS composition requires a design phase.

We deduce that WS composition may be much more complex than composing Telecom-services, so that cannot be automated in general. To address the complexity of WS composition, in several models, those have been developed, such as orchestration and choreography.

Now, let us draw the attention of the reader to an important difference between Telecom-services and WSs in FI detection. The presence of FIs between the two composed Telecom-services depend generally unique on those composed services, because the composition consists simply in running the services in parallel. On the contrary, the presence of FIs in WSs depends generally on the way of the WSs have been composed, because there are many ways to compose WSs.

3. Related Work on Modeling and Composing WSs and Detecting Their FIs

An important contribution[13, 14] is to raise the interest of researchers to the problem of WS composition and FI detection[13]. That presents a case of study which can be used as a benchmark to assess FI detection methods. Another contribution in raising an interest can be found in[15], which shows that FIs of Telecom-Services are different from FIs in WSs.

Let the term *on-line* (resp. *off-line*) qualify the methods which are applicable during in the *execution* (resp. *design*). On-line WS composition and FI detection methods are studied for example in[18-20]. [18]presents an on-line of FI detection method inspired from the *Situation of Calculus*. [19]presents an on-the-fly approach to compose WSs. [20]identifiy some challenges and opportunities in on-line FI detection and resolution.

Much more work has been done in off-line WS composition and FI management, *e.g.* in[21-25]. [21]proposes an off-line FI detection method using *Label Transitions Systems* (LTS). [22]proposes a method based on Petri nets that detects one type of FIs: *race conditions*. [23]uses Petri nets to describe WSs and presents simple examples for merging WS descriptions. [24]presents an FI detection method using the model-checker UPPAAL; WSs are described in WS-BPEL which is translated into *timed automata*. [25]presents an FI detection method that uses the *model-checker* SPIN[26]; WSs are described in BPEL4WS[27] which is translated into Promela.

Some work on user-interfacing and software-tooling for WS composition can be found in[28, 29]. [28]proposes an environment using *Mashup* for WS composition, and[29] presents an integrated development environment for WS composition. FI detection is not studied in [28, 29].

[30, 31]propose an extension of the business model of[32] to support WS composition. The authors of[30, 31] go further in[33] by studying how WSs can be categorized and assembled. FI detection is not studied in[30, 31, 33].

[34, 35]contain a rigorous study of WS composition, where theoretical, software-tooling and user-interfacing aspects are considered. The CRESS formalism is used which can be automatically translated into BPEL and LOTOS.

4. Use-Modify Language to Model WSs

In the references of Section 3 that study FI detection, the developed FI detection methods may suffer from state space explosion, because they are based on formalisms specifying WS behaviors exhaustively. The approach we adopt targets to avoid state space explosion while keeping an acceptable power of FI detection. For that purpose, we develop a so-called Use-Modify language (or UM-language) to model WSs at a high abstraction level, whose principle is to specify "who uses what" and "who modifies what". Such an omission of details is motivated by the desire to avoid state space explosion during FI detection. With Use-Modify, WSs are specified at two levels: their *interfaces* are specified like objects in object-oriented analysis (OOA); and their *behaviors* are specified by what called is Use-Modify relations (UM-relations) in the form of "L uses of Y" or "L modifies to R". L and R correspond to WSs, functionalities of WSs or variables of WSs, and either "use" and "modification" are characterized by "always", "sometimes", "never" or "maybe". A set of UM-relations modeling the behavior of the WS is called its behavior model, or its UM-model to emphasize the use of UM-relations. The UM-model describes a WS *logically*, in the sense that it specifies how a WS behaves but it does not necessarily to correspond to its implementation. The UM-model is targeted uniquely to be manipulated by our proposed FI detection method which will be presented in Section 6. While designing (and pre deploying) a WS, a UM-model of such a WS must be constructed and analyzed to determine whether the WS is FI prone. Therefore, our method is off-line.

4.1. Interface Model Based on Object-Oriented Analysis

The interface of a WS is modeled as a class skeleton in OOA, and the interface of each executable instance of WS is modeled as an object skeleton of a class. By *skeleton*, we mean that the classes and objects are specified by attributes and methods *signatures*. A method signature specifies a function by its name, its input and/or output parameters and its returned result (if any), and *without* a body. Object skeleton corresponds to interface in Java. Hence, the behavior is not specified. For the sake of brevity, we will omit the terms *skeleton* and *signature* in *class skeleton*, *object skeleton*, and *method signature*. There exist two types of attributes: *basic attributes* and *complex attributes*. Basic attributes are variables of primitive types, like int, float, double, boolean. Complex attributes are objects. For the sake of clarity, methods, basic attributes and complex attributes are named differently as follows:

- Basic attributes (or primitive variables): they are named in italic with the first letter non capitalized. For example, *risk*, *rate*, and *amount*.
- Complex attributes (or objects): they are named in italic with the first letter capitalized. For example, *Assessor*, *Approver*, *Lender*, *Supplier*.
- Methods: they are named in italic with the first letter non capitalized, and they terminate by ().For example, *quote*(), *approve*() and *assess*().

As in OOA, attribute *a* and a method *m*() of an object *O* are referred to as *O.a* and *O.m*(), respectively. The object name *O* can be omitted when there is no ambiguity or when it is irrelevant. We will use the notions of feature and WS as follows:

- Feature: it is a basic WS which is not composed of other WSs. A feature is modeled as

  an object whose all attributes are basic. When several similar features are used, the latter can be modeled as objects of the same class. A class is named with all letters capitalized, for example, *SUPPLIER*.
- WS: it is a complex WS created by composing features and/or WSs. Like features, WSs can be modeled by objects and classes. The fact that a WS is composed of several objects (WSs and/or features) implies that it has a complex attributes.

Let us consider some examples of features and WSs taken from [35] and give an idea of how they can be modeled as objects. We do not present them in detail, we just indicate one or two attributes and methods for each feature or WS.

Example 1: The feature *Approver* has a method *approve*() and two basic attributes *amount* and *rate*. *approve*() evaluates a loan of a given *amount* and refuses or approves it. A *rate* is selected if the loan is approved.

Example 2: The feature *Assessor* has a method *assess*() and three basic attributes *amount*, *risk* and *rate*. *assess*() evaluates the *risk* of a loan of a given *amount*. If *risk* is low, an acceptation response is returned with a proposed loan *rate*, otherwise a refusal is returned.

Example 3: The WS *Lender* is composed of the two features *Approver* and *Assessor*. *Lender* has two attributes that correspond to *Approver* and *Assessor*. *Lender* has also a method *quote*() and a basic attribute *amount*. The method *quote*() approves or assesses a loan of a given *amount* in the following way: *quote*() invokes the method *approve*() of *Approver* if *amount* ≥ 10000, or the method *assess*() of *Assessor* if *amount* < 10000. *quote*() also invokes *approve*() if *assess*() returns a refusal.

We have shown how WSs have their interfaces (and not their behaviors) modeled as classes and objects. Note that these interfaces can be visualized as a subset of UML class diagrams where the unique associations are compositions and aggregations, which may seem too restrictive compared to UML class diagrams. This restriction is justified by the fact that our interfaces will be used uniquely to detect FIs at a high abstraction level. These interfaces do not reflect necessarily the implementation structures of WSs, while UML class diagrams can be used to model implementations, and hence may need to be closely associated to implementations structures.

Interfaces do not give any information on how WSs behave. In the above three examples, the behaviors were indicated for information, they are not described in the objects. In the remainder of Section 4, we show how WSs have their behaviors modeled at a high abstraction level by the Use-Modify formalism.

4.2. Introduction to the Use-Modify Formalism

A method is said *active* if its execution modifies (sometimes or always) the value of some attribute (of any object). An object is said *active* if it contains an active method or a complex attribute which is an active object. A basic attribute cannot be active. A method or object is said *passive* if it is not active. Intuitively, an active object is an object that permits to modify some attribute (of any object). Let *active access* to an attribute mean an access that modifies the attribute. Hence, we categorize accesses in two actions: “use” and “modify” which will be characterized by various “intensities”. Let us first consider the “use” of the action:

- “use!” means “has *always* access to”.

- "use?" means "has *sometimes* access to"; by sometimes, we mean under some specified or unspecified conditions which happen to be true (i.e. the conditions cannot be always false).
- "use%" means "has *never* access to".
- "use#" means "has *maybe* access to", i.e., we do not know if there is an access.

In the same way, the action "modify" is used with various "intensities" as "modify!", "modify?", "modify%" and "modify#". The difference between "use" and "modify" is that "modify" corresponds to an active access, while "use" corresponds to an access which may be passive or active.

To clarify particularly the semantics of "always", "sometimes", "maybe" and "never", we detail below the different types of so-called Use-Modify relations (or UM-relations):

"L use! R" means that R is accessed each time and L is applied.

"L use? R" means that R is accessed in *some* (known or unknown) situation(s) where L is applied. Note that this case may include the following two cases:

- L has access to R in some situations not in all situations;
- L has access to R in all situations.

"L use% R" means that L never uses R.

"L use# R" means that we suspect that L uses R, but we are not certain.

"L modify! R" strengthens "L use! R" by specifying that the access is active, *i.e.* R is modified each time L is applied.

"L modify? R" strengthens "L use? R" by specifying that the access is active, *i.e.* R is modified in *some* (known or unknown) situation(s) where L is applied. Note that this case may include the following two cases:

- L modifies R in some situations not in all situations;
- L modifies R in all situations.

"L modify% R" means that L never modifies R.

"L modify# R" means that we suspect that L modifies R, but we are not certain.

Note that use# is less precise than use!, use? and use%, and modify# is less precise (we also say: weaker) than modify!, modify! and modify%. use# and modify# have been defined and we will show that if they can be deduced by some rules. Typically, a UM-relation "L use# R" is irrelevant (hence of that should be removed) so if we have one of its stronger UM-relations "L use! R", "L use? R" or "L use% R". In the same way, a UM-relation "L modify# R" is irrelevant (so that should be removed) if we have one of its stronger UM-relations "L modify! R", "L modify? R" or "L modify% R". We will return to this aspect in Section 5.6.3.

In the sequel, "!", "?", "%" and "#" are not written in some contexts where they are irrelevant. In this case, we write "use" to mean "use!", "use?", "use%" or "use#", and we write "modify" to mean "modify!" or "modify?", "modify%" or "modify#".

4.3. Well-formed UM-relations "L use R" and "L modify R"

In this subsection, we still clarify more the semantic of UM-relations "L use R" and "L modify R" and we present restrictions on R and L that are necessary and sufficient to characterize a UM-relation as well-formed.

4.3.1. UM-relation "L use R"

In a UM-relation "L use R":

- R can be a method *m*(): "L use *m*()" means that L calls *m*();
- R can be a basic attribute *x*: "L use *x*" means that L reads or changes the value of *x*.
- R can be a complex attribute, i.e. R is an object which may have its own (basic and complex) attributes and/or methods:

"L use R" means that L uses one or more of the attributes or methods of R.

In the above three cases, we have the actions "calls", "reads or changes" and "uses", respectively. We refer to any of these actions by "action on R". The 3 cases are generic since we have "use" without !, ?, # or %. Let us see what we obtain if we replace the generic "use" by use!, use?, use# or use? :

- With use! : we have to characterize the action on R by "always",
- With use? : we have to characterize the action on R by "sometimes",
- With use#: we have to characterize the action on R by "maybe",
- With use%: we have to characterize the action on R by "never".

Let us now see the conditions on L in a UM-relation "L use R":

- L can be a method *p*(): the action on R is realized by the execution of *p*().

- L can be a complex attribute: there are two possible situations:
  - L has a method that realizes the action on R;
  - L has a complex attribute that realizes the action on R.
- L cannot be a basic attribute: indeed, a basic attribute can uniquely be read and modified.

4.3.2. UM-relation "L modify R"

A difference with "L use R" is that in "L modify R", R cannot be a method, because it is a nonsense to modify a method. The latter can uniquely be called (i.e. used). Hence, in a UM-relation "L modify R":

- R cannot be a method *m*(): a method can only be used (by calling it);
- R can be a basic attribute *x*: "L modify *x*" means that L changes the value of *x*.
- R can be a complex attribute, i.e. R is an object which may have its own (basic and complex) attributes and/or methods:
  "L modify R" means that L modifies one or more of the attributes or methods of R.

In the above two "can be" cases, we have the actions "changes" and "modifies", respectively. We refer to any of these actions by "active action on R". The 2 cases are generic since we have "modify" without !, ?, # or %. Let us see what we obtain if we replace the generic "modify" by modify!, modify?, modify# or modify? :

- With modify! : we have to characterize the active action on R by "always",
- With modify? : we have to characterize the active action on R by "sometimes",
- With modify#: we have to characterize the active action on R by "maybe",
- With modify%: we have to characterize the active action on R by "never".

The conditions on L in a UM-relation "L modify R" are the same conditions identified for "L use R" in Subsection 4.3.1.

Definition 4.1 *(Well-formed UM-relation)* A UM-relation "L use R" (resp. "L modify R") is said well-formed if it respects the conditions of Subsection 4.3.1 (resp. 4.3.2).

4.4. Examples of UM-models

Example 4: Here are some UM-relations that can be derived from the literal descriptions in Examples 1, 2, 3 of Section 4.1:

Approver (of example 1):

M1: *Approver.approve*() modify! *Approve.amount* // *approve*()
// sets *amount* by a value received as input argument

M2: *Approve*r*.approve*() modify? *Approver.rate* //*approve*() computes
//*rate* if loan accepted

Assessor (of example 2):

M3*:* *Assessor.assess*() modify! *Assessor.amount* // *assess*() sets *amount*
// by a value received as input argument

M4: *Assessor.assess*() modify! *Assessor.risk* // *assess*() computes the
//*risk*

M5: *Assessor.assess*() modify? *Assessor.rate* //*assess*() computes the
//*rate* if the *risk* is low

Lender (of example 3): Since *Lender* is composed of *Approver* and *Assessor*, its model contains the UM-relations M1-M5. Additional UM-relations are necessary to model the coordination of Approver and Assessor by Lender. Here are examples of such additional UM-relations:

M6: *Lender* use! *Lender.quote*() // *Lender* starts by the execution of
//its method *quote*()

M7: *Lender.quote*() modify! *Lender.amount* // *quote*() sets *amount* by a
//value received as input argument

M8: *Lender.quote*() use? *Approver.approve*() // *quote*() calls *approve*()
// if *amount* $\geq$ 10000 or if *assess*() refuses the loan

M9: *Lender.quote*() use? *Assessor.assess*() // *quote*() calls *assess*() if
// *amount* < 10000

Example 5: Let us use the benchmark of [13] to present other examples of use? and modify?. Examples 5, 6 and 7 of this benchmark are related to accessing the user profile. We consider a WS *Supplier* that needs to have access to user profiles. We assume that each profile contains two parts: a confidential part and a public part. The two parts can be read and modified by the profile of the owner. The confidential part can also be read by some trusted entities, while the public part can be read by anyone.

All what concerns a user is represented as an object *User* with an attribute *profile*. The latter represents the user profile which is itself an

object with two attributes *conf* and *pub*, for the confidential and public parts respectively. Here are some UM-relations
where *Supplier* is a trusted or untrusted supplier.

N1: *Supplier* use? *User.profile* // *Supplier* can read *profile* with the
// following restriction: *Supplier* can read the confidential
//part only if he is trusted.

N2: *Supplier* modify% *User.profile* // *Supplier* cannot modify
//*profile*

N3: *Supplier* use? *User.profile.conf* // *Supplier* can read *conf*
//only if he is trusted

N4: *Supplier* modify% *User.profile.conf* // *Supplier* cannot modify
//*conf*

N5: *Supplier* modify% *User.profile.pub* // *Supplier* cannot modify
// *pub*

4.5. Conditions Associated to UM-Relations

In a UM-relation "L x R", we may specify conditions as follows:

L x R : [condition1, condition2, …]

Consider for example a WS *Supplier* to which an order can be sent, *e.g.*, by calling its method *order*()). *Supplier* can itself call the *order*() method of another supplier of the same class *SUPPLIER*. This is specified by the UM-relation "*Supplier.order*() use? *SUPPLIER.order*()". Assuming a supplier does not call its own *order*() method, we associate to this UM-relation a condition stating that *SUPPLIER* does not comprise *Supplier*. Formally:

Supplier.order() use? *SUPPLIER.order*() : [*SUPPLIER* ≠ *Supplier*].

This condition will be reconsidered in the example of Section 7.1.

Conditions can also be useful in a UM-relation with "use?" or "modify?" to justify why we have not "use!" or "modify!" in the considered UM-relation. Consider for example a supplier who accesses some information in the profile of a customer only if he is authorized. This can be modeled as follows:

Supplier use? *profile* : [*Supplier.authorized* = true].

This kind of condition will be used to define a FI pattern, namely Pattern 4 of Section 6.3. It will be illustrated by an example in Section 7.5.

5. Logical Rules of Use-Modify Language

To make UM-modeling applicable in a rigorous way, we provide in this section a set of logical rules that can be used in the phase of construction of UM-relations modeling a WS or several interacting WSs. We will consider three types of rules:

- *implication UM-rules*: they permit to deduce a new UM-relation from an existing UM-relation;
- *fusion UM-rules*: they permit to deduce a new UM-relation from two existing UM-relations;
- *contradiction UM-rules*: they permit to identify incompatible UM-relations.

Let us first give in Section 5.1 fundamental rules from which the three types of UM-rules will be synthesized in Sections 5.2-5.4. By fundamental, we mean that the rules of Section 5.1 are based on general logical statements; they do not refer directly to UM-relations. Sections 5.5-5.6 are related to soundness and completeness of the fundamental and UM-rules. Section 5.7 illustrates the use of UM-rules.

5.1. Fundamental rules

The objective of this subsection is to identify a set of fundamental rules that specify:

- links between "use" and "modify" (R_1, R_2);
- links between "always", "sometimes" and "never (R_3-R_5);
- How "use" can be combined with other actions by transitivity (R_6-R_9).

Note that these rules are not specified formally because their objective is to present fundamental principles which will justify the formal rules of Sections 5.2-5.4.

5.1.1. Links between "use" and "modify"

The action "use" refers to any active or passive access. That is, "L uses R" means that L has an access to R which may or may not modify the state of R. The action "modify" is an active "use", *i.e.* "L modifies R" means that L has a particular use of R that modifies its state. Hence, L can modify R only by using it, or in other terms, L cannot modify R if L does not use R. therefore we have the following two rules R_1 and R_2 which are in fact equivalent:

R_1 : "L modifies R" implies "L uses R";

R_2 : "L does not use R" implies "L does not modify R".

5.1.2. Links between "always", "sometimes" and "never"

In Section 4.2, we have explained our exact semantics of "always", "sometimes", "never" and "maybe", from which the following rules R_3-R_5 can be easily understood. Note that "maybe" does not intervene in these rules; this is because our semantics of "maybe" is too coarse and corresponds to a "don't know" situation.

R_3 : "L always makes an action A" implies "L sometimes makes A";

R_4 : "L never makes an action A" and "L sometimes makes A" are contradictory;

R_5 : "L never makes an action A" and "L always makes A" are contradictory.

5.1.3. Combining "use" with other actions by transitivity

Consider actors U, L and R, such that U always applies an action A to R. Our semantics of "always" (Section 4.2) means that each time U is used, it inevitably applies the action A to R. Consider the following two cases:

- Assume that L sometimes uses U, *i.e.* there is at least one case where L uses U. Hence, we deduce logically that there is at least one case where L applies the action A to R, *i.e.* L sometimes applies the action A to R. This leads to rule R_6 below.
- Assume that L always uses U, *i.e.* each time L is used, it uses U. Hence, we deduce logically that each time L is used it applies the action A to R, *i.e.*, L always applies the action A to R. This leads to rule R_7 below.

Assuming that U always applies the action A to R:

R_6: "L sometimes uses U" implies "L sometimes applies A to R";

R_7: "L always uses U" implies "L always applies A to R".

Consider now actors U, R and L, such that U sometimes applies an action A to R. Our semantics of "sometimes" (Section 4.2) means that there is at least one case where U applies the action A to R. Consider the following two cases:

- Assume that L sometimes uses U, *i.e.* there is at least one case where L uses U. We cannot deduce anything about the application of A by L, for the following reason: the cases where U applies A to R are not necessarily the cases where L uses U. Hence, we can only deduce that L maybe applies action A to R, which corresponds to rules R_8.
- Assume that L always uses U, *i.e.* each time L is used, L uses U. We cannot deduce anything about the application of A by L, for the following reason: the cases where U applies A to R are not necessarily the cases where L is used. Hence, we can only deduce that L maybe applies action A to R, which corresponds to rules R_9.

Assuming that U sometimes applies the action A to R:

R_8: "L sometimes uses U" implies "L maybe applies A to R";
R_9: "L always uses U" implies "L maybe applies A to R".

5.1.4. Recapitulation of the fundamental rules R_1-R_9

R_1 : "L modifies R" implies "L uses R".
R_2 : "L does not use R" implies "L does not modify R".
R_3 : "L always makes an action A" implies "L sometimes makes A".
R_4 : "L never makes an action A" contradicts "L sometimes makes A".
R_5 : "L never makes an action A" contradicts "L always makes A".
Assuming that U always applies an action A to R:
R_6: "L sometimes uses U" implies "L sometimes applies A to R";
R_7: "L always uses U" implies "L always applies A to R".
Assuming that U sometimes applies an action A to R:
R_8: "L sometimes uses U" implies "L maybe applies A to R";
R_9: "L always uses U" implies "L maybe applies A to R".

From R_1-R_9, we define in Sections 5.2-5.4 three types of specific UM-rules (*i.e.* rules on UM-relations): implication UM-rules, fusion UM-rules, and contradiction UM-rules. These UM-rules are identified in the form I_n, F_n and C_n, respectively, and also in a mnemonic form **R[…]** that may help to guess the statement of each rule.

5.2. Implication UM-Rules

In this subsection, we present implication UM-rules, *i.e.* we identify cases where a UM-relation implies another UM-relation. The implication UM-rules I_1-I_5 below are deduced from Rules R_1-R_3 of Section 5.1. More precisely:

- I_1 and I_2 are the translations of R_1 into UM-rules by characterizing the actions by “always” and “sometimes”, respectively.
- I_3 and I_4 are the translations of R_3 into UM-rules by using the actions “modify” and “use”, respectively.
- I_5 is the translation of R_2 into UM-rule.

The condition associated to I_5 is required to guarantee that the derived “L modify%” is well-formed assuming that “L use%” is well-formed. This condition is necessary because the “well-formed” constraints of “L use% R” (in Subsection 4.3.1) are weaker than the “well-formed” constraints of “L modify%” (in Subsection 4.3.2). The UM-rules I_3-I_4 do not require conditions because the “well-formed” constraints of their left members are the same as the “well-formed” constraints of their right members. The UM-rules I_1-I_2 do not require conditions because the “well-formed” constraints of their left members are stronger than the “well-formed” constraints of their right members.

I_1 : R[m!=>u!]: “L modify! R” => “L use! R”
I_2 : R[m?=>u?]: “L modify? R” => “L use? R”
I_3 : R[m!=>m?]: “L modify! R” => “L modify? R”
I_4 : R[u!=>u?]: “L use! R” => “L use? R”

Assuming that the conditions of Section 4.3.2 are respected by L and R:

I_5 : R[u%=>m%]: “L use% R” => “L modify% R” if the condition of

5.3. Fusion UM-Rules

In this subsection, we present fusion UM-rules, *i.e.* we identify cases where two UM-relations derive another UM-relation. The fusion rules F_1-F_4 below are deduced from Rules R_6-R_7 of Section 5.1.3 as follows:

- F_1 is the translation of R_7 into UM-rule by taking action A as “use R”,
- F_2 is the translation of R_6 into UM-rule by taking action A as “use R”,

- F_3 is the translation of R_7 into UM-rule by taking action A as "modify R".
- F_4 is the translation of R_6 into UM-rule by taking action A as "modify R",

The UM-rules F_5-F_8 below are deduced by combining I_1-I_2 and F_1-F_4 as follows:

- F_5 is deduced from I_1 and F_1,
- F_6 is deduced from I_2 and F_2,
- F_7 is deduced from I_1 and F_3,
- F_8 is deduced from I_2 and F_4.

F_1 : **R[u!u!=>u!]**: "L use! U" and "U use! R" => "L use! R"
F_2 : **R[u?u!=>u?]**: "L use? U" and "U use! R" => "L use? R"
F_3 : **R[u!m!=>m!]**: "L use! U" and "U modify! R" => "L modify! R"
F_4 : **R[u?m!=>m?]**: "L use? U" and "U modify! R" => "L modify? R"
F_5 : **R[m!u!=>u!]**: "L modify! U" and "U use! R" => "L use! R"
F_6 : **R[m?u!=>u?]**: "L modify? U" and "U use! R" => "L use? R"
F_7 : **R[m!m!=>m!]**: "L modify! U" and "U modify! R" => "L modify! R"
F_8 : **R[m?m!=>m?]**: "L modify? U" and "U modify! R" => "L modify? R"

The UM-rules F_9-F_{12} below are deduced from R_8-R_9 of Section 5.1.3 as follows:

- F_9 is the translation of R_9 into UM-rule by taking action A as "use R",
- F_{10} is the translation of R_8 into UM-rule by taking action A as "use R",
- F_{11} is the translation of R_9 into UM-rule by taking action A as "modify R",
- F_{12} is the translation of R_8 into UM-rule by taking action A as "modify R".

Note that F_9 and F_{11} can also be deduced as follows:

- F_9 is deduced from I_4 and F_{10},
- F_{11} is deduced from I_4 and F_{12}.

We have also the UM-rules F_{13}-F_{16} which can be deduced as follows:

- F_{13} is deduced from I_1 and F_9,
- F_{14} is deduced from I_2 and F_{10},
- F_{15} is deduced from I_1 and F_{11},
- F_{16} is deduced from I_2 and F_{12}.

Note that F_{13} and F_{15} can also be deduced as follows:

- F_{13} is deduced from I_3 and F_{14},
- F_{15} is deduced from I_3 and F_{16}.

F_9 : **R[u!u?=>u#]**: "L use! U" and "U use? R" => "L use# R"

F_{10} : **R[u?u?=>u#]**: "L use? U" and "U use? R"=> "L use# R"

F_{11} : **R[u!m?=>m#]**: "L use! U" and "U modify? R" => "L modify# R"

F_{12} : **R[u?m?=>m#]**: "L use? U" and "U modify? R" => "L modify# R"

F_{13} : **R[m!u?=>u#]**: "L modify! U" and "U use? R" => "L use# R"

F_{14} : R[m?u?=>u#]: "L modify? U" and "U use? R" => "L use# R"

F_{15} : **R[m!m?=>m#]**: "L modify! U" and " U modify? R" => "L modify# R"

F_{16} : **R[m?m?=>m#]**: "L modify? U" and "U modify? R" => "L modify# R"

5.4. Contradiction UM-Rules

In this subsection, we present contradiction UM-rules, *i.e.* we identify pairs of UM-relations which are incompatible (or mutually exclusive) with each other. A UM-model containing pairs of incompatible UM-relations is inconsistent and hence may be a symptom of FI. The four contradiction UM-rules C_1-C_4 below are deduced from Rule R_4-R_5 of Section 5.1.2 as follows:

- C_1 is the translation of R_4 into UM-rule, by taking action A as "modify R",

- C_2 is the translation of R_4 into UM-rule, by taking action A as "use R",
- C_3 is the translation of R_5 into UM-rule, by taking action A as "modify R",
- C_4 is the translation of R_5 into UM-rule, by taking action A as "use R".

Note that C_3 and C_4 can also be deduced as follows:

- C_3 is implied from I_3 and C_1,
- C_4 is implied from I_4 and C_2.

We have also the UM-rules C_5-C_6 which can be deduced as follows:

- C_5 is implied from I_5 and C_1 and from I_2 and C_2,
- C_6 is implied from I_5 and C_3, I_1 and C_4, also from I_3 and C_5.

C_1 : R[m? ≠ m%]: "L modify? R" and "L modify% R" => Incompatibility

C_1 : R[m? ≠ m%]: "L modify? R" and "L modify% R" => Incompatibility

C_2 : R[u? ≠ u%]: "L use? R" and "L use% R" => Incompatibility

C_3 : R[m! ≠ m%]: "L modify! R" and "L modify% R" => Incompatibility

C_4 : R[u! ≠ u%]: "L use! R" and "L use% R" => Incompatibility

C_5 : R[m? ≠ u%]: "L modify? R" and "L use% R" => Incompatibility

C_6 : R[m! ≠ u%]: "L modify! R" and "L use% R" => Incompatibility

5.5. Soundness and Completeness Results

Note that R_1-R_3, R_6-R_9, I_1-I_5 and F_1-F_{16} derive new UM-relations from existing UM-relations, while R_4-R_5 and C_1-C_6 detect incompatibilities between UM-relations. We will use the symbol wrt for "with regard to". We will also use "logically" to mean "by using reasoning based on 1^{st}-order logic.

Proposition 5.1 *(Preservation of "well-formed")* Each of the UM-rules I_1-I_5 and F_1-F_{16} derives a well-formed UM-relation when its left hand side member (one or two UM-relations) is well-formed. (Well-formed is defined in Section 4.3.).

Definition 5.1 *(Soundness)***:** Consider a set R of rules applicable to UM-relations. R is said sound (implicitly wrt 1^{st}-order logic), if for every set K of UM-relations, all UM-relations and incompatibilities between UM-relations that can be deduced by R from K can also be deduced logically. Intuitively, soundness of R is that R is a subset of the 1^{st}-order logic.

Definition 5.2 *(Completeness wrt rules)***:** Consider two sets F and R of rules applicable to UM-relations. R is said complete wrt F, if for every set K of UM-relations, all UM-relations and incompatibilities between UM-relations that can be deduced by F from K can also be deduced by R. Intuitively, completeness of R wrt F is that F is a subset of R.

Definition 5.3 *(Completeness)***:** Consider a set R of rules applicable to UM-relations. R is said complete if it is complete wrt 1^{st}-order logic. Intuitively, R is complete if it implies all the UM-relations and incompatibilities between UM-relations that can be implied logically (*i.e.* by 1^{st}-order logic).

Proposition 5.2 *(Soundness)***:** The set of UM-rules {I_1-I_5, F_1-F_{16}, C_1-C_6} is *sound.*

Proposition 5.3 *(Completeness wrt* R_1-R_9*)***:** The set of UM-rules {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_2} is *complete* wrt R_1-R_9.

5.6. Discussion

5.6.1. Relation of soundness and completeness with FI detection

Soundness is stated in Proposition 5.2 for {I_1-I_5, F_1-F_{16}, C_1-C_6}, while Proposition 5.3 states completeness of only a subset of {I_1-I_5, F_1-F_{16}, C_1-C_6}. The question is:

Why soundness and completeness are not stated for the same set of UM-rules ?

Or more precisely:

Why soundness is stated for {I_1-I_5, F_1-F_{16}, C_1-C_6} while it can be stated for the subset {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_2} which is proved to be sound and complete ?

Our answer is developed in the following paragraph.

In fact, we can use uniquely the set of UM-rules {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_2} and base our FI detection on this set. The problem is that we have realized by experience that the UM-rules I_1-I_5 may imply much more UM-relations than what is necessary for our FI detection. Hence, there is the risk to undermine significantly the efficiency of our FI detection procedure. By combining the results of Sections 5.3-5.4, it is easy to see that F_5-F_8, F_{13}-F_{16} and C_3-C_6 are implied by combining I_1-I_5 with {F_1-F_4, F_9-F_{12}, C_1-C_2}. Interestingly, we have realized by experience that I_1-I_5 are indeed relevant for our FI detection only to be combined with {F_1-F_4, F_9-F_{12}, C_1-C_2} to derive what can be derived by the missing UM-rules F_5-F_8, F_{13}-F_{16} and C_3-C_6. Our strategy is therefore to adapt the complete set {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_2} by removing I_1-I_5 and adding F_5-F_8, F_{13}-F_{16} and C_3-C_6. We obtain {F_1-F_{16}, C_1-C_6} which is the set of UM-rules which are used for our FI detection. Intuitively, this is equivalent to using the complete set {I_1-I_5, F_1-F_{16}, C_1-C_6}, but by applying I_1-I_5 only to derive UM-relations which may be relevant for our FI detection.

5.6.2. About soundness of R_1-R_9

Completeness stated by Proposition 5.3 is wrt R_1-R_9. Intuitively, every UM-relation and incompatibility between UM-relations that is implied from R_1-R_9 can also be implied from {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_2}. A question that arises is: *Is {I_1-I_5, F_1-F_8, C_1-C_4} complete (Def. 5.3) ?* The answer to this question is Yes if R_1-R_9 is complete. Hence, another question that arises is: *Is R_1-R_9 complete ?* At the present time, we have not a formal answer to this question, but it is worth noting that our development of R_1-R_9 has been dictated by the desire to obtain a sound set of rules which is as much complete as possible. Let us give some explanations to clarify this aspect. Recall that UM-relations are based on:

1) actions “use” and “modify”, and
2) characterizing each action by “always”, “sometimes”, “never” or “maybe”.

The development of R_1-R_9 has been dictated as follows:

- R_1-R_2 are related to point 1: they targets to specify as much as possible the distinction between actions “use” and “modify”.
- R_3-R_5 are related to point 2: they target to specify as much as possible the distinction between “always”, “sometimes” and “never”. “maybe” is not considered because it is a too coarse information which does not permit any deduction.
- R_6-R_9 target to derive *logically* new UM-relations by combining existing UM-relations.

R_6-R_7 consider the cases where an action is followed by "use!" or "modify!", while R_8-R_9 consider the cases where an action is followed by "use?" or "modify?".
The two cases are distinguished because R_8-R_9 are too coarse since they imply a
UM-relation with an action "use#" or "modify#" (see Section 5.1.3).

5.6.3. Utility of use# and modify#

One may wonder why "maybe" characterization (use#, modify#) has been used although it represents a too coarse information. In fact, a UM-relation "L x# R" (where x is "use" or "modify") is clearly irrelevant if there exists a UM-relation with the same L, R and x, but where x is characterized by !, ? or % instead of #. For example, "A use# B" is irrelevant if we have "A use? B", "A use! B" or "A use% B". Otherwise, we will see in Sect. 6 that "L x# R" may be relevant in FI detection to model a suspected FI.

5.7. Example of Using UM-rules to Derive new UM-Relations

Example 6: Consider Example 4 of Sect. 4.4 and apply some UM-rules to the UM-relations M1-M9. We obtain the following UM-relations that enrich the UM-model of *Lender*.

Applying F_3 to M6 and M7 : *Lender* modify! *Lender.amount*
Applying F_4 to M8 and M1 : *Lender.quote*() modify? *Approver.amount*
to M9 and M3 : *Lender.quote*() modify? *Assessor.amount*
Applying F_9 to M6 and M8 : *Lender* use# *Approver.approve*()
to M6 and M9 : *Lender* use# *Assessor.assess*()
Applying F_4 to M9 and M4 : *Lender.quote*() modify? *Assessor.risk*
Applying F_{12} to M8 and M2 : *Lender.quote*() modify# *Approver.rate*
to M9 and M5 : *Lender.quote*() modify# *Assessor.rate*

In this example, the suspected accesses (use#, modify#) deduced from F_9 and F_{12} are effective, hence we have a more accurate model if we replace "use#" by "use?" and "modify#" by "modify?". We have not shown the influence of conditions in the application of rules; we will illustrate their influence in FI detection in Sects. 7.1 and 7.5.

6. FI Detection Method Based on UM-Relations

As already mentioned, there exist many FI detection methods with a high power of detection, but which are prone to state space explosion. In this section, we propose an FI detection method that reduces this problem while keeping an acceptable power of FI detection. The approach is off-line and consists in detecting FIs in a WS during its design (from scratch or by composing existing WS). More precisely, the approach consists in constructing a UM-model of the WS under design, and then in analyzing such a UM-model to detect FI patterns which correspond to symptoms of FI. The designer is informed about each detected symptom and should check if it corresponds to an effective FI. This necessity of the intervention of the designer implies that the FI detection procedure is not completely automatic. This is the price to pay to reduce the state space complexity.

The proposed FI detection method consists of three steps. The first step is to construct a UM-model of the WS under design. The second step is to check if the UM-model is well-formed (*i.e.* all its UM-relations are well-formed) and to enrich it. The third step is to analyze the UM-model to detect symptoms of FIs. The three steps are presented in Sections 6.1-6.3 respectively.

Definition 6.1 *(F-relevance)* A pair of UM-relations is said $F_{1\text{-}8}$-relevant if it can be a left hand side member of a fusion UM-rule of F_1-F_8. A pair of UM-relations is said $F_{9\text{-}16}$-relevant if it can be a left hand side member of a fusion UM-rule of F_9-F_{16}.

6.1. Step 1: UM-Model Construction

Let **S** be the WS under design. The first step can be skipped if the UM-model of **S** already exists and is given as input to the second step (Section 6.2). Otherwise, we have the following two different cases, which are presented in Sections 6.1.1 and 6.1.2.
respectively:

- **S** is designed from scratch, .i.e. **S** is a feature (see Sect. 4.1) ;
- **S** is designed by composing several given WSs S_1, S_2, …, S_n.

6.1.1. Step 1 when S is designed from scratch

We consider that the designer has defined on paper the UM-model of **S**. The first level of the model is an interface model (Section 4.1) which consists of a class with empty methods. Since **S** is a feature (basic WS), the attributes of the class are basic. The second level is a UM-model consisting of UM-relations "L x R", where L and R are object(s) of the class defined in the first level, or attributes or methods of that object(s), as shown in Sections 4.2-4.5. The designer edits the UM-model, for example with any text editor or some UM-editor which is specifically designed to edit interactively UM-models.

6.1.2. Step 1 when S is designed by composing WSs S_1, S_2, ..., S_n

We consider that UM-models S_1, S_2, …, S_n are given as inputs of Step 1, for example in text files. The designer has access to these UM-models, for example with any text editor or some specific UM-editor. With the available editor, the designer has to construct a UM-model which merges the UM-models of S_1, S_2, …, S_n. Some treatments may have to be done in the obtained UM-model. Typically, a treatment consists in removing, adding and/or replacing a UM-relation. The treatment is for example used to model the coordination of the composed WSs. The result of merging and treatment is the UM-model of **S**. To understand the necessity of treatment, consider for example the composition of two WSs S_1 and S_2 by choreography. Each of S_1 and S_2 may have to call methods of the other one. Hence, the composition of S_1 and S_2 may require that the designer applies some modifications to S_1 and/or S_2 by removing, adding and/or replacing some UM-relation(s). The modified UM-relations should be indicated (*e.g.* by a flag), because the modifications may be a cause of FI and thus should be considered in the phase of FI detection (in Section 6.3, Step 3, Pattern 3).

6.2. Step 2: Verifying that the UM-Model of S is well-formed and Enriching it

This step is divided in the following three substeps which will be explained and justified in their corresponding sections:

- *Substep 2a*: checking if each UM-relation of the UM-model is well-formed, as specified in Section 4.3;

- *Substep 2b*: enriching the UM-model by applying the UM-rules F_1-F_8 of Sections 5.3;
- *Substep 2c*: enriching the UM-model by applying the UM-rules F_9-F_{16} of Sections 5.3.

Substeps 2b and 2c are used separately, because F_9-F_{16} derive UM-relations with actions use# and modify# and require a specific treatment as explained in Section 5.6.3.

Substeps 2a-2c will be illustrated by the following example of UM-model, where the UM-relations are identified by r_i, *m*() is a method, and *v* is a basic attribute:

r_1 :	U	use!	V
r_2 :	U	use%	V
r_3 :	V	modify!	W
r_4 :	U	modify%	W
r_5 :	X	use?	U
r_6 :	W	use?	Z
r_7 :	X	use!	Z
r_8 :	L	modify?	*m*()
r_9 :	*v*	use!	R

6.2.1. Substep 2a: verifying if all UM-relations are well-formed

The constraints specified in Section 4.3.1 are checked for each UM-relation "L use R", and the constraints specified in Section 4.3.2 are checked for each UM-relation "L modify R". At the end of the procedure (outlined below), the returned set X contains all UM-relations detected as non-well-formed. We consider that the subsequent steps cannot be executed while the returned X is not empty. Hence, when X is not empty, the designer must correct the non-well-formed UM-relations and re-execute Substep 2a until the returned X is empty. As in Step 1 (Section 6.1.2), the correction should be indicated (*e.g.* by a flag), because it may be a cause of FI and thus should be considered in the phase of FI detection (in Section 6.3, Step 3, Pattern 3).

Procedure to find the non-well-formed UM-relations
Input: R = set of UM-relations obtained after Step 1
Result: X = set of non-well-formed UM-relations of R
BEGIN

X := empty set
for each UM-relation A of R **:**
| **if** (A is non-well-formed)
| |insert A in X I have not used “move A to X” because I do not want to remove A from R
| **end-if**
end-for
return X
END

For our example, the UM-rule r_8 is non-well-formed because in “L modify R”, R can be a basic or complex attribute, it cannot be a method (see Section 4.3.2). A method is used (by calling it), it cannot be modified. Another non-well-formed UM-rule is r_9 because in “L x R”, L cannot be a basic attribute; the latter can be used or modified, it cannot use or modify. We consider here that the adopted solution is to remove the non-well-formed r_8 and r_9. This may require adapting the WS **S** under design.

6.2.2. Substep 2b: enriching the UM-model by applying F_1-F_8

In Section 5.6.1, we have explained why we will use only the set of UM-rules {F_1-F_{16}, C_1-C_6}. In fact, the present substep 2b uses F_1-F_8, while substep 2c uses F_9-F_{16}. The UM-rules C_1-C_6 will be used in Step 3, more precisely in Pattern 5 of Section 6.3.

The UM-model R of **S** is enriched “maximally” by synthesizing *all* the new UM-relations that are implied by the UM-rules F_1-F_8. By “maximally”, we mean “iteratively until no new UM-relation is derived”. This can be realized by a fix-point method which iterates the UM-rules F_1-F_8 until no new UM-relation is generated. The method converges because of the *finite* numbers of rules (F_1-F_8) and actions (use!, use?, use%, modify!, modify?, modify%). The structure of the iterative method is shown below.

Explanations of the procedure below: Its input R is the current set of UM-relations. Its result is an enriched R, i.e. R with additional UM-relations derived by applying fusion UM-rules F_1-F_8. F contains the set of $F_{1\text{-}8}$-relevant pairs of UM-relations of R which have not yet been treated as a left hand side member of a fusion UM-rule to derive a new UM-relation. Hence, F is initialized as the set of all $F_{1\text{-}8}$-relevant pairs of UM-relations of R. The simplest approach to construct F consists in considering every UM-relation A of R and comparing it with every other UM-relations B of R to determine if the pair (A, B) is the left hand side member of a fusion UM-rule in F_1-F_8. If yes, the pair is inserted in F. The while-loop generates all the new UM-relations that can be derived by applying the UM-rules F_1-F_8 to the pairs of UM-relations of F. At each while-iteration, we select some pair of F, and the objective is to apply the fusion UM-rule F that has as left hand side member. Let B be the UM-relation derived by F. If B is not already in R, it is inserted in R (because R must contain all derived UM-relations). The for-loop consists in updating F by comparing B with every other UM-relation U of R and to insert the pair (B,U) in F if it is $F_{1\text{-}8}$-relevant (to treat (B,U) in a subsequent while-iteration, as a left hand side member of a UM-rule to try to derive a new UM-relation). Then, the pair is removed from F when it has been treated.

```
Procedure to enrich the UM-model R by using F1-F8:
Input:   R = set of UM-relations obtained after Substep 2a
Result: Enriched R
BEGIN
   F := set of all F1-8-relevant pairs of UM-relations of R
   while (F is not empty):
    |  select some pair    of F
    |  let F be the fusion UM-rule having    as left hand side member
    |  let B be the UM-relation which is the right hand side member of F
    |  if  (B is not in R) :
    |   |    insert B in R
    |   |    for every UM-relation U in R
    |   |     |   if (B,U) is F1-8-relevant:  insert (B,U) in F
    |   |    end-for
    |  end-if
    |  remove the pair    from F
   end-while
END
```

For our example, the UM-relations r_8 and r_9 were removed in Step 2a and the UM-model R after Substep 2a is { r_1, …, r_7}. The set of $F_{1\text{-}8}$-relevant pairs is F = {(r_1, r_3), (r_5, r_1)}. The two pairs of F are left hand side members of UM-rules F_3 and F_2 respectively. Let us execute the procedure to this example.

1st iteration: by applying F_3 to (r_1, r_3), the following new UM-relation r_{10} is derived:

r_{10}: "U modify! W"

r_{10} is inserted in R; its addition implies the new $F_{1\text{-}8}$-relevant pair (r_5, r_{10}) which is inserted to F. The treated pair (r_1, r_3) is removed from F. Hence, we obtain R = {r_1, …, r_7, r_{10}} and F = {(r_5, r_1), (r_5, r_{10})}.

2nd iteration: by applying F_2 to (r_5, r_1), the following new UM-relation r_{11} is derived:

r_{11}: "X use? V"

r_{11} is inserted in R; its addition implies the new $F_{1\text{-}8}$-relevant pair (r_{11}, r_3) which is inserted in F. The treated pair (r_5, r_1) is removed from F. Hence, we obtain R = { r_1, …, r_7, r_{10}, r_{11}} and F = {(r_5, r_{10}), (r_{11}, r_3)}.

3rd iteration: by applying F_4 to (r_5, r_{10}), the following new UM-relation r_{12} is derived:

r_{12}: "X mod? W"

r_{12} is inserted in R; its addition implies no new $F_{1\text{-}8}$-relevant pair. The treated pair (r_5, r_{10}) is removed from F. Hence, we obtain R = { r_1, …, r_7, r_{10}, r_{11}, r_{12}} and F = {(r_{11}, r_3)}.

4th iteration: by applying F_4 to from (r_{11}, r_3), the existing UM-relation r_{12} is derived. The treated pair (r_{11}, r_3) is removed from F which becomes empty, and hence the while-loop terminates. We obtain R = { r_1, …, r_7, r_{10}, r_{11}, r_{12}}.

6.2.3. Substep 2c: enriching the UM-model by applying F_9-F_{16}

We proceed with a similar procedure as in Substep 2b, except that:

- we consider UM-rules F_9-F_{16} instead of F_1-F_8;
- every new derived UM-relation "L use# R" or "L modify# R" is removed if the UM-model of **S** contains a UM-relation with the same L, R and x, but where x is characterized by !, ? or % instead of # (see Section 5.6.3).

For our example, the set of UM-relations after Substep 2b is R = {r_1, …, r_7, r_{10}, r_{11}, r_{12}}. The set of $F_{9\text{-}16}$-relevant pairs is F = {(r_3, r_6)}, where (r_3, r_6) is a left hand side member of the UM-rule F_{13}. Let us execute the procedure to this example.

1st iteration: by applying F_{13} to (r_3, r_6), the following new UM-relation r_{13} is derived:

r_{13}: "V use# Z"

r_{13} is inserted in R, its addition implies no new $F_{9\text{-}16}$-relevant pair. The treated pair (r_3, r_6) is removed from F which becomes empty, and hence the while-loop terminates. R_{13} is not removed from R because R contains none of "V use! Z", "V use? Z" and "V use% Z". Hence, after Step 2c we obtain R = { r_1, …, r_7, r_{10}, …, r_{13}}.

6.3. Step 3: FI Detection

Step 3 is the proper FI detection procedure. We have identified six FI patterns that represent symptoms (hence potentiality) of FIs. The procedure of Step 3 searches FI patterns in the UM-model R obtained in Step 2, and informs the designer about every detected FI pattern to draw his attention on the corresponding suspected FI. The designer should then react by making adequate verifications. The six identified FI patterns are presented below. For each FI pattern, we indicate a typical reaction of the designer to determine whether the FI is effective or not.

Pattern 1. There exists a "reflexive" UM-relation "*a*() use! *a*()" or "*a*() use? *a*()" or "*a*() use# *a*()", where *a*() is a method. This is a symptom of *looping behavior* which is illustrated by the example of Section 7.1.

Reaction of the designer: the designer should check whether there is an effective looping behavior with action *a*():

Pattern 2. There exist UM-relation(s) that "modify" and possibly "use" the same entity. That is, two or more UM-relations "K m R" and "L n R" are detected, where m is any "modify*" other than "modify%", and n is any "use*" or "modify*" other than "use%" and "modify%". This is a symptom of *resource conflict* or *race condition* which is illustrated by the examples of Sections 7.4, 7.7, 8.1, 8.2, 8.3.

Reaction of the designer: the designer should check whether there exists an effective conflicting access to R.

Pattern 3. There exist UM-relation(s) obtained (in Step 1 and/or Step 2a) by correcting (removing, adding and/or replacing) UM-relation(s) of S_1, …, S_n. There is hence the possibility that an identified correction may violate requirements of S_1, …, S_n the designer has in mind, hence the *potentiality* of FI . This case is illustrated by the example of Sect. 7.2.

Reaction of the designer: the designer should check whether the identified.
corrections violate requirements.

Pattern 4. There exist UM-relation(s) with restrictions. By the generic term "restriction", we mean any of the following two situations:

- There exist UM-relations "L use? R" or "L modify? R" which are associated to specified conditions (Section 4.5).
  Reaction of the designer: the designer should check that the specified conditions are respected.
- There exist UM-relation(s) "L use% R" or "L modify% R".
  Reaction of the designer: the designer should check that for every "L use% R", R is effectively never used by L; and for every "L modify% R", R is effectively never modified by L.

The two sub-cases of Pattern 4 are illustrated in Section 7.5 with use? and modify%.

Pattern 5. There exist incompatible UM-relations. We have actually two types of incompatibilities:

- Two UM-relations "A use* *p*()" and "A use* *q*()", where * may be "!" or "?", and *p*() and *q*() are methods which are incompatible with each other. Here, we assume that in the UM-model R, the designer has specified pairs of incompatible methods.
  For example, this can be formally expressed as follows: for each method *p*() having incompatible methods, we specify the set {q_1(), q_2(), …} of methods which are incompatible with *p*() by:
  Incompatible[*p*()] = q_1(), q_2(), …
  This case is illustrated by the example of Section 7.3.
- Two UM-relations which are incompatible by the contradiction UM-rules C_1-C_6 (Section 5.4).
  Incompatibilities are symptoms of *inconsistent behavior*.

Reaction of the designer: the designer should check that any detected incompatibility really exists.

Pattern 6. Forbidden UM-relation(s) are present or mandatory UM-relation(s) are missing. Here, we assume that in the UM-model R, the designer has specified forbidden UM-relation and mandatory UM-relations. For example, this can be formally expressed as follows:

Each mandatory (resp. forbidden) UM-relation is followed at its right by the keyword Mandatory (resp. Forbidden). This case is illustrated by the examples of Sections 7.2 and 7.6.

Reaction of the designer: the designer should check whether the detected forbidden UM-relations really occur, and whether the missing mandatory UM-relations really do not occur.

Note that we consider only FI detection and not FI resolution. As we have shown, when an FI is detected and reported to the designer, his reaction is to determine if the FI is effective. A further step (left for future work) is to determine how to correct the UM-model to eliminate the detected FIs.

6.4. Results and Discussion on Computational Complexity

The development of the UM-based FI detection method has been motivated by the desire to reduce state space explosion. The approach has been that instead of modeling a feature or WS exhaustively by representing many of its states and transitions, we model only certain of its behaviors and properties that are judged relevant. Those relevant behaviors and properties are in the form of UM-relations which themselves are based on objects and their attributes and methods. Two questions arise:

a) How to identify relevant behaviors and properties?
b) How to quantify the reduction of complexity by this approach?

Point a) requires designers who have much experience in designing web services or more generally software services. The designers must also have a good knowledge of the specifications of the WS under design. We have used “designers” in the plural because we think that a good approach to guarantee a good estimation of relevant behaviors and properties is the well-known principle of *diverse design*. The principle is that the same specification of the WS under design is given to several teams who proceed independently to design different versions of UM-models of the WS. Then, the resulting multiple versions are compared with each other to detect their differences. Finally, the teams discuss with each other to agree on a common UM-model. A good example of successful application of diverse design can be found in [36] for firewall design.

About Point b), we have studied the computational complexity of the three steps of FI detection (of Sections 6.1-6.3). The obtained results are given by the following proposition (its proof is in Section 10.4).

Proposition 6.1 *(Complexity of the three steps of FI detection)*:
Let S_1, …., S_n be the WSs to be composed and nbR_1, …, nbR_n be the sizes (*i.e.* numbers of UM-relations) of their respective UM-models.
The computational complexity of Step 1 is in $O(nbR_1+\ldots+nbR_n)$.
The computational complexity of Step2 is in $O((nbR_1+\ldots+nbR_n)^6)$.
The computational complexity of Step 3 is in $O((nbR_1+\ldots+nbR_n)^4)$.

In the case of a single WS (i.e., WS designed from scratch), the above results hold by taking a single nbR instead of a sum $nbR_1+\ldots+nbR_n$.

Let us discuss the results of Proposition 6.1 in comparison to the complexities obtained with more exhaustive models such as those based on automata.

- The exponents 4 and 6 in some results of Prop. 6.1 may seem excessive, but it is worth noting that these are theoretical upper bounds which are very far from the concrete results we have obtained in real examples. The latter are not higher than $O((nbR_1+\ldots+nbR_n)^2)$. Even in the theory, it may be impossible to reach complexity with exponents 4 and 6, because our complexity study has been quite permissive as it can be seen in the proof of Prop. 6.1.
- About a basic WS, i.e. not composed of other WSs: with our experience, we expect that the size of an automaton modeling a basic WS should be at least 10 times higher than the size of a UM-model of such a basic WS.
- About a complex WS, i.e. composed of several WSs: the sizes of the composed UM-models are *summed*, instead of being *multiplied* as it is the case with automata-based models. Such a multiplication is the main cause of the well-known state space explosion problem.

7. Demonstration of FI Detection in the Benchmark of [13] and in an Example of [14]

Let us demonstrate our FI detection method in the examples of the benchmark of [13]. The latter contains the case study of a fictitious virtual bookstore on which is constructed a benchmark of eight FIs. The following *individual* WSs are defined:

iPassport is an *identity management* WS that simplifies authentication with multiple
service providers.

PayMe is a *payment processing* WS that allows payers to make secure payments online, and simplifies credit card processing for payees.

ShipEx is a *shipping* WS that provides shippers with guaranteed delivery of product, and simplifies tracking of a shipment for shipees.

Shark is a *caching* WS that improves performance by storing the results of previous requests.

Then, three *composite* WSs ***Amazin***, ***Supplier*** and ***Customer*** are constructed from the above individual WSs. ***Amazin*** is a *virtual bookstore* which relies on a number of ***Suppliers***, and gives ***Customers*** access to its virtual catalog and the option to order books from the catalog through an ***Order Processing*** feature.

7.1. Example 1 of[13]: Called "OrderProcessing – OrderProcessing"

The FI manifests itself by a blocking situation in the following way. An order is sent to $Supplier_1$ (by calling a method *order*() of $Supplier_1$) who forwards the order to $Supplier_2$ (by calling a method *order*() of $Supplier_2$) because his stock is empty. Then, $Supplier_2$ in turn decides to forward the order to $Supplier_1$ (by calling a method *order*() of $Supplier_1$) because his stock too is empty too. Hence, we reach the blocking situation where each supplier is waiting the reception of the ordered book from the other supplier. Let us see how our FI detection method detects such FI. The UM-models of $Supplier_1$ and $Supplier_2$ contain respectively the following UM-relations with conditions, as seen in Section 4.5:

UM1: "$Supplier_1$.*order*() use? *SUPPLIER.order*()" : [*SUPPLIER not comprising* $Supplier_1$],

UM2: "$Supplier_2$.*order*() use? *SUPPLIER.order*()" : [*SUPPLIER not comprising* $Supplier_2$].

The UM-models models of $Supplier_1$ and $Supplier_2$ are composed (Step 1) and the resulting UM-model is enriched (Step 2). In Step 2c, the UM-rule F_{10} is applied to UM1 and UM2, but after setting *SUPPLIER* of UM1 and UM2 to $Supplier_2$ and $Supplier_1$, respectively; we obtain:

UM1-UM2: "$Supplier_1$.*order*() use# $Supplier_1$.*order*()".

Hence, FI pattern 1 is detected in Step 3. Note that this scenario can be generalized to a loop involving more than two suppliers: *Supplier*$_1$ is waiting *Supplier*$_2$ who is waiting *Supplier*$_3$ … *Supplier*$_k$ who is waiting *Supplier*$_1$.

7.2. Example 2 of [13]: Called "Caching – Process Payment"

The FI manifests itself by the fact that, if an ordered book is in the cache (because it has been previously purchased), then the process payment is shortcut. Hence, the order is completed without payment. Let us see how our FI detection method detects such an FI. *Supplier* and *Caching* WSs are specified by a set of UM-relations. Consider a method *completeOrder*() which is called in *Supplier* when everything is ready to start payment and delivery processes. The payment process starts by calling a method *pay*(). A UM-relation which is particularly relevant in this example is: *completeOrder*() use! *pay*()

The UM-models of *Supplier* and *Caching* are composed (Step 1) and the resulting UM-model is enriched (Step 2). This example illustrates the situation where composing two WSs requires that the designer modifies the process payment of *Supplier* as explained above. The present composition has the effect to replace the call of a method *pay*() by a conditional call. Hence the above UM-relation is replaced by the UM-relation *completeOrder*() use? *pay*()" (i.e., "use!" replaced by "use?"). Hence, FI pattern 3 is detected in Step 3.

Another way to detect the FI is that the designer specifies the UM-relation "*completeOrder*() use! *pay*()"as mandatory. The FI is deduced by the fact that the composition has modified this mandatory UM-relation. Hence, the FI pattern FI pattern 6 is detected in Step 3.

7.3. Example 3 of [13]: Called "Order Processing – (Delivery or Process Payment)"

We consider two situations of FI that may occur when the order of a book is aborted (before its completion). These two FIs are referred to as **(a)** and **(b)** as follows:

(a) FI Called "Order Processing – Delivery" in [13]: The FI manifests itself when, due to timing errors, a process payment is aborted while the delivery is completed (instead of being aborted). Hence, the possibility to receive a book which has not been paid (as in Example 2, but for a different reason).

(b) FI Called "Order Processing - Process Payment" in [13]: The FI manifests itself when, due to timing errors, a delivery is aborted while the process payment is completed (instead of being aborted). Hence, the possibility to pay for a book which is not received.

Let us see how our FI detection method detects such FIs. A supplier WS is composed of several features such as: *ProcessPayment*, *Delivery*, and *OrderProcessing*, each one being described by UM-relations. The different UM-models are composed (Step 1) to obtain a UM-model of *Supplier* which is enriched (Step 2).

The UM-model of *Supplier* uses the following methods: *abortOrder*() is called to abort the current order, *pay*() is called to start payment for the ordered product, and *deliver*() is called to start delivery of the ordered product. *abortOrder*() is incompatible with *deliver*() and *pay*(), because payment and delivery must not be done when an order is aborted. We assume that the designer has specified these incompatibilities.

The UM-model contains the following three UM-relations:

R1: "*Supplier* use? *abortOrder*()", R2: "*Supplier* use? *deliver*()", R3: "*Supplier* use? *pay*()"

Hence, the FI pattern FI pattern 5 is detected in Step 3 for the pairs (R1,R2) and (R1,R3). The incompatible pair (R1, R2) corresponds to FI (a), and the incompatible pair (R1, R3 corresponds to FI (b).

7.4. Example 4 of [13]: Called "Order Processing - Fulfill Order"

The FI considered here is due to an ambiguity on the semantics of the price. More precisely, the FI manifests itself when some features use the term price, but assigning it different semantics. For example, one feature considers the price *including* taxes, while another feature considers the price *excluding* taxes. Let us see how our FI detection method detects such FI. The UM-model and Steps 1 and 2 are as in Example 3 (Section 7.3). After steps 1 and 2 The UM-model of *Supplier* uses two methods *orderProcessing*() and *fulfillOrder*() that modify an attribute *price*, *i.e.* we have the following UM-relations:

"*orderProcessing*() modify? *price*" "*fulfillOrder*() modify? *price*"

Hence, FI pattern 2 is detected in Step 3.

7.5. Examples 5, 6, 7 of[13]: All Associated to Access Profile

We consider Examples 5, 6 and 7 together, because they correspond to several variants of the same problem: *non respecting the profile access policy*. Intuitively:

- **In example 5** (called "Authenticate User - Access profile" in [13]): an untrusted supplier accesses some information in the profile of the customer.
- **In example 6** (called "Access Profile - Access profile" in [13]): a trusted supplier accesses some information in the profile of the customer, which must be accessible uniquely to the customer.
- **In example 7** (called "Manage Profile - Access profile" in [13]): a supplier accesses some information in the profile of the customer when the latter is not connected.

After Steps 1 and 2, the resulting UM-model contains UM-relations such as:

"*Supplier* use? *profile*" : {*Supplier* is authorized}
"*Supplier* modify% *profile*"

Hence, FI pattern 4 is detected in Step 3. Note the condition {*Supplier* is authorized} associated to the first UM-relation, which models the fact that only the authorized suppliers can read a user profile. The "modify%" corresponds to the restriction specifying that no supplier is authorized to modify a user profile. Hence, the designer should check if these restrictions are respected. The FIs of Examples 5, 6 and 7 are due to the non-respect of some authorizations.

7.6. Example 8 of[13]: Called "Order Processing - Order Processing"

The FI manifests itself by a blocking situation where $Supplier_1$ is waiting $Supplier_2$ who in turn is waiting $Supplier_1$, which corresponds exactly to Example 1 (Section 7.1). Hence Examples 1 and 8 are identical, but in Example 8, the FI is presented with a different viewpoint: *None of the suppliers is available to the other one.* A way to detect this FI is given in Section 7.1. Let us present another way to detect this FI.

We assume that the designer has specified the following UM-relation as forbidden: "*Supplier* modify? *available*",
where "available" is a boolean that indicates whether Supplier is available or not. Intuitively, *Supplier* cannot make himself unavailable.

The fact is that after Steps 1 and 2, the resulting UM-model will contain the above forbidden UM-relation.

Hence, FI pattern 6 is detected in Step 3, which is a symptom that availability changes and hence *available* can be false in some situations.

7.7. Example of[14]: Called "Spell Checking - Formatting"

The FI manifests itself when the *Spell Checker* and the *Formatter* use different languages, *e.g*., US English and UK English. At the formal level, this FI is similar to the FI of Example 4. In the latter, two methods modify an attribute *price*. In the present example, two features *SpellChecker* and *Formatter* modify an attribute *lang* specifying the used language. After Steps 1 and 2, the resulting UM-model contains the following UM-relations: "*SpellChecker* modify? *lang*" "*Formatter* modify? *lang*".

Hence, FI pattern 2 is detected in Step 3.

8. Demonstration in Detection of Several FIs of [15]

[15] presents an interesting comparative study showing that FIs in Telecom-Services are different from FIs in WSs, and hence FI detection methods developed for the former cannot be easily adapted for the latter. We will apply our FI detection to three types of FIs given in [15]:

- FI between two WSs;
- FI between two Telecom-services;
- FI between a WS and a Telecom-service.

As we will see, the three FIs are related to FI pattern 2 of Step 3.

8.1. FI Between Two WSs of [15]: "Encrypt Information – Payment Information"

The FI manifests itself when the *Logging* WS uses the encrypted information (purchase order or payment information) while *Logging* needs to use the information *before* it is encrypted. After Steps 1 and 2, we obtain UM-relations where an attribute *paymentInfo* is modified by a method *encrypt*(), while another method *logging*() reads the attribute *paymentInfo*. That is, we have the following UM-relations:

"*encrypt*() modify! *PaymentInf*o" "*logging*() use! *PaymentInfo*"

Hence, FI pattern 2 is detected in Step 3.

8.2. FI Between Two Telecom-Services of [15]: "Voicemail (VM) – Call Blocking (CB)"

Contrary to previous examples, here we consider Telecom-services instead of WSs. The FI manifests itself when a caller rejected by *Call-Blocking* (*CB*) of a callee is able to leave a (potentially unwanted) voicemail via *Voicemail* (*VM*). After Steps 1 and 2, we obtain UM-relations where an attribute *callStatus* is modified by *CB* (to busy status) and read by *VM* (busy status is the trigger of VM). That is, we have the following UM-relations:
"*CB* modify! *callStatus*" "*VM* use! *callStatus*".
Hence, FI pattern 2 is detected in Step 3.

8.3. FI Between a Telecom-Service and a WS of [15]: "Talk-To-Agent (TTA) – Do-Not-Disturb (DND)"

This is a special case, in the sense that we have a *mixed* composition, *i.e.*, a WS is composed with a Telecom-service. The FI manifests itself when a customer wants to be joined by an agent to talk with him (WS called *TTA*), while he has configured the Telecom-service Do-Not-Disturb (*DND*) to reject all calls. After Steps 1 and 2, we obtain UM-relations where the attribute *callStatus* (already used in the example of Section 8.2) is modified by *DND* (to the status busy, for example) and read by a method *tta*(). That is, we have the following UM-relations: "*DND* modify! *callStatus*", "*tta*() use! *callStatus*". Hence, FI pattern 2 is detected in Step 3.

9. Conclusion

We have developed a method to detect FIs in WSs, which makes a trade-off between reducing state space explosion and increasing the power of FI detection. The proposed method is based on the development of a rigorous Use-modify framework. The latter contains a UM-language to describe WSs at a high abstraction level by objects and UM-relations which indicate uniquely information such as who uses what and who modifies what, and characterize each action "use" or "modify" by "always", "sometimes", "never" or "maybe". Conditions and restrictions may also be associated to UM-relations. In addition to the UM-language, the UM-framework contains also a set of UM-rules (*i.e*. rules applicable to UM-relations) that are proved to be sound and complete. The UM-rules permit to derive new UM-relations from existing UM-relations and detect incompatibilities between UM-relations. The developed UM-based FI detection method reports FI symptoms to the designer who then has to verify the effectiveness of the suspected FIs.

We have demonstrated the applicability of our FI detection method in several concrete examples. Indeed, we have applied our method to detect all FIs of the benchmark of [13] and an FI in [14]. We have also applied our method to detect several FIs indicated in [15], where the composed services can be WSs and/or telecommunication services. We think that our FI detection approach can be better than [13] because in the latter many modeling formalisms have to be used: Goal-oriented Requirement Language (GRL), Use-Case Maps (UCM), and Finite State Processes (FSP).

In Section 6.4, we have briefly discussed the gain in computational complexity of our UM-based approach. In a near future work, we plan to study more thoroughly that complexity. For that purpose, we plan to develop a prototype of the UM-based FI detection method to evaluate it more accurately. Another planned future work is to study FI *resolution* phase, which consists in solving the detected FIs.

10. Proofs

10.1. Proof of Proposition 5.1

We have to prove that the UM-rules I_1-I_5 and F_1-F_{16} preserve the well-formed property specified in Section 4.3 (for I_1-I_5, see also the explanations in Section 5.2).

The well-formed property is preserved by I_1-I_2 because for any I_1 or I_2, the well-formed property requires stronger constraints on the left hand side of the UM-rule than on its right hand side.

The well-formed property is preserved by I_3-I_4 because for any I_3 or I_4, The well-formed property requires the same constraints on the left and right hand sides of the UM-rule.

The well-formed property is preserved by I_5 because of the condition associated with I_5.

The well-formed property is preserved by F_1-F_4 because for any of F_1 to F_4: The "well-formed" constraints on L are the same in the left and right hand sides of the UM-rule; and the "well-formed" constraints on R are the same in the left and right hand sides of the UM-rule.

The well-formed property is preserved by F_5 (resp. F_7) because it is obtained by combining I_1 with F_1 (resp. F_3) which have just been proved to preserve the well-formed property. In the same way, the well-formed property is preserved by F_6 (resp. F_8) because it is obtained by combining I_2 with F_2 (resp. F_4) which have just been proved to preserve the well-formed property.

The well-formed property is preserved by F_9-F_{16} because we can make the same reasoning as with F_1-F_8. ■

10.2. Proof of Proposition 5.2

We have to prove that the set of UM-rules {I_1-I_5, F_1-F_{16}, C_1-C_6} is sound. We will use the term "logically" to mean "by using reasoning based on 1^{st}-order logic".

The set of rules R_1-R_9 is sound because every rule R_1 to R_9 has been justified *logically* in Section 5.1 .

In Section 5.2, we have shown that the implication UM-rules I_1-I_5 are direct

translations of rules R_1-R_3.

In Section 5.3, we have shown that the fusion UM-rules F_1-F_4 are direct translations of rules R_6-R_7, and F_9-F_{12} are direct translations of rules R_8-R_9.

In Section 5.4, we have shown that the contradiction UM-rules C_1-C_4 are direct translations of rules R_4-R_5.

Consequently, the set of UM-rules {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_4} is a direct translation of the set of rules R_1-R_9. Since R_1-R_9 is sound, we deduce that its translation {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_4} is sound.

In Section 5.3, we have shown that F_5-F_8 are derived *logically* from I_1-I_2 and F_1-F_4, and that F_{13}-F_{16} are derived *logically* from I_1-I_2 and F_9-F_{12}. In Section 5.4, we have shown that C_5-C_6 are derived *logically* from {I_1-I_5, C_1-C_4}. Since F_5-F_8, F_{13}-F_{16} and C_5-C_6 are derived logically from UM-rules of {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_4} which has just been proved to be sound, we have that the whole set {I_1-I_5, F_1-F_{16}, C_1-C_6} is sound. ■

10.3. Proof of Proposition 5.3

We have to prove that the set of UM-rules {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_2} is *complete* wrt R_1-R_9.

We have shown in Sections 5.2-5.4 and in the proof of Proposition 5.2 that the set of UM-rules {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_4} is a direct translation of the set of rules R_1-R_9. Moreover, in Sections 5.2-5.4, the UM-rules {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_4} have been obtained by considering all possible translations of R_1-R_9 into UM-rules. In other words, {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_4} are the unique possible translations of R_1-R_9 into UM-rules. Therefore, R_1-R_9 and {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_4} imply the same UM-relations and detect the same pairs of incompatible UM-relations. Besides, we have seen in Section 5.4 that C_3-C_4 can be implied *logically* from I_3-I_4 and C_1-C_2. Hence, C_3 and C_4 can be omitted in the study of completeness. Consequently, R_1-R_9 and {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_2} imply *logically* the same UM-relations and incompatibilities between UM-relations. In other words, {I_1-I_5, F_1-F_4, F_9-F_{12}, C_1-C_2} is *complete* wrt R_1-R_9. ■

10.4. Proof of Proposition 6.1

Let S_1, …., S_n be the WSs to be composed and nbR_1, …, nbR_n be the sizes (i.e. numbers of UM-relations) of their respective UM-models. For simplicity of notation, we use *nbR* to denote $nbR_1+\ldots+nbR_n$.

10.4.1 Computational complexity of Step 1

- Merging all UM-relations: its complexity is in the order of the total number of all number of UM-relations, i.e. O(*nbR*).
- Modifying UM-relations: in the worst case, all UM-relations are modified, which is in the same order as merging, i.e. O(*nbR*).
- Adding some UM-relations: the number of added UM-relations is typically quite less than the total number of UM-relations, i.e. its order is smaller than O(*nbR*).

Therefore, we obtain that in Step 1 the computational complexity and the number of UM-relations is in O(*nbR*).

10.4.2 Computational complexity of Step 2

2a: Check if each UM-relation is well-formed

Its complexity is in the order of the number of UM-relations obtained in Step 1, i.e. O(*nbR*).

2b. Enriching the UM-model by applying F_1-F_8

Let |X| denote the size (or cardinality) of a set X.
Let R_i and R_f be the set R of UM-relations before and after Step 2, respectively (indices i and f are for initial and final). Recall that $O(|R_i|) = O(nbR)$ (result of Step 1).

Each UM-relation of R_f has:

- its left hand side member as a left hand side member of some UM-relation of R_i ;
- its right hand side member as a right hand side member of some UM-relation of R_i.

Hence, at the maximum, for each of the left hand side members of UM-relations of R_i, we may associate any of the right hand side members of UM-relations of R_i. That is, we may have at the maximum nbR^2 UM-relations in R_f. Consequently, the size of R after Step 2 is upper-bounded by $O(nbR^2)$, i.e. $O(|R_f|) = O(nbR^2)$.

Let us consider the algorithm that constructs R_f from R_i.
Let F_i be the initial F constructed just before the while-loop.

During the execution of this algorithm, we define:

- *q* as the number of times a UM-relation is inserted in R ;
- *p* as the number of times a pair of UM-relations is inserted in F ;
- *k* as the number of times a pair of UM-relations is removed from F.

We have:

- *q* is in the order of $|R_f|$, and we have seen that $O(|R_f|) = O(nbR^2)$. Hence, $O(q) = O(nbR^2)$.

- F_i contains pairs of UM-relations of R_i, and we have seen that $O(|R_i|) = O(nbR)$. Hence, $O(|F_i|)= O(|R_i|^2) = O(nbR^2)$.
- Each of the q times where a UM-relation is inserted in R, we may have pairs of UM-relations inserted in F (in the for-loop). The number of these pairs is at most in the order of the current size of R, which is at most $O(|R_f|)$ which was shown to be $O(nbR^2)$. Hence, $O(p) = O(|R_f| \text{x } q) = O(nbR^4)$, because it has been shown that $O(|R_f|) = O(nbR^2)$ and $O(q) = O(nbR^2)$.
- $|F_i| - k + p = 0$ (i.e. $k = |F_i| + p$), because F is empty at the termination of the algorithm. Since it has been shown that $O(|F_i|)= O(nbR^2)$ and $O(p) = O(nbR^4)$, we conclude that $O(k) = O(nbR^4)$.

We have shown that the number k of iterations of the while-loop is upper-bounded by nbR^4. At each of the k iterations of the while-loop:

- the complexity for checking the condition of "if" is upper-bounded by $O(|R_f|) = O(nbR^2)$ because at most, B is compared to every UM-relation of the current R. The complexity of all other statements is in O(1).
- The number of iterations of the for-loop is in $O(|R_f|) = (nbR^2)$

Hence, the complexity of the algorithm (i.e. Step 2b) is upper-bounded by $O(nbR^4 \text{ x } nbR^2) = O(nbR^6)$.

2c: Enriching the UM-model by applying F_9-F_{16}

Applying F_9-F_{16} has its complexity in the same order as that of Step 2b, i.e. upper-bounded by $O(nbR^6)$.

Recall that the size of R after Step 2b (and also Step 2c) is in $O(nbR^2)$.

Removing irrelevant UM-relations:

- Searching UM-relations "L use# R" or "L modify# R": in $O(nbR^2)$.
- For each found UM-relation: searching a more accurate UM-relation: in $O(nbR^2)$.

Hence, removing irrelevant UM-relations is upper-bounded by $O(nbR^4)$.

Therefore, Step 2c is in $O(nbR^6)$.

Therefore, the total complexity of Step 2 is upper-bounded by O(nbR^6).

10.4.3 Computational complexity of Step 3

Recall that O(nbR^2) is the order of the size of R after Step 2.

We compute the complexity for each pattern:

Pattern 1: Detecting "reflexive" UM-relations "*m*() use* *m*()", where * is ?, ! or # (i.e. * is not %). It is in the size of R : O(nbR^2).

Pattern 2: Detecting two or more UM-relations "K m R" and "L n R", where m is any "modify*" other than "modify%", and n is any "use*" or "modify*" other than "use%" and "modify%". It is in the square of the size of R : O(nbR^4).

Pattern 3: Detecting UM-relation(s) modified in Step 1. It is in the size of R : O(nbR^2).

Pattern 4: Detecting UM-relation(s) with restrictions. It is in the size of R : O(nbR^2).

Pattern 5: Detecting incompatible UM-relations. Since we have to consider pairs of UM-relations, the complexity is in the square of the size of R : O(nbR^4).

Pattern 6: Let *nbM* and *nbF* be the numbers of UM-relations specified as mandatory and forbidden, respectively.

Verifying the presence of mandatory UM-relations: for each mandatory UM-relation M, we go through the UM-relations of R to verify the presence of M. Hence, the complexity is at most in *nbM* multiplied by the size of R, i.e. O($nbM \times nbR^2$).

Verifying the absence of the forbidden UM-relations: for each forbidden UM-relation F, we go through the UM-relations of R to verify the presence of F. Hence, the complexity is at most in *nbF* multiplied by the size of R, i.e. O($nbF \times nbR^2$).

Hence, the total complexity of Pattern 6 is in O($(nbM + nbF) \times nbR^2$).

Typically, the total number ($nbM + nbF$) of mandatory and forbidden UM-relations is smaller than the size of R, *i.e.* $O(nbM + nbF) < O(nbR^2)$. Therefore, the complexity of Pattern 6 is upper-bounded by $O(nbR^4)$. Hence, the total computational complexity of the three steps: $O(nbR^6)$.

References

[1] **Bouma, L.G** and **Velthuijsen, H.** (eds), *Feature Interactions in Telecom. Systems*, IOS Press, Amsterdam (1994).

[2] **Cheng, K.E.** and **Ohta, T.** (eds), *Feature Interactions in Telecom. Systems III*, IOS Press, Amsterdam, (1995).

[3] **Dini, P**, **Boutaba, R.** and **Logrippo, L.** (eds), *Feature Interactions in Telecom. Networks IV*, IOS Press, Amsterdam (1997).

[4] **Kimbler, K.** and **Bouma, L.G.** (eds), *Feature Interactions in Telecom. and Software Systems V,* IOS Press, Amsterdam (1998).

[5] **Calder, M.** and **Magill, E.** (eds), *Feature Interactions in Telecom. and Software Systems VI*, IOS Press, Amsterdam (2000).

[6] **Amyot, D.** and **Logrippo, L.** (eds), *Feature Interactions in Telecom. and Software Systems VII*, IOS Press, Amsterdam (2003).

[7] **Reiff-Marganiec, S.** and **Ryan, M.** (eds), *Feature Interactions in Telecom. and Software Systems VIII*, IOS Press, Amsterdam (2005).

[8] **du Bousquet, L.** and **Richier, J.L.** (eds), *Feature Interactions in Software and Communication Systems IX,* IOS Press, Amsterdam (2007).

[9] **Nakamura, M.** and **Reiff-Marganiec, S.** (eds), *Feature Interactions in Software and Communication Systems X*. IOS Press, Amsterdam (2009).

[10] **Kimbler, K.**, EURESCOM Project P509 Handling Service Interactions in the Service Life Cycle, Retrieved: April 1, 2011 from http://www.eurescom.de/~public-seminars/1997/IN/P509a (1998).

[11] **Chentouf, Z.**, Detecting OAM&P Design Defects Using a Feature Interaction Approach, *Int. Journal of Network Management,* **22**(2):95-103 (2012).

[12] **Khoumsi, A.**, **Chentouf, Z.** and **Qasem, S.**, A High Abstraction Level Approach for detecting Feature Interactions in Web Services, *IADIS Int. Conf. e-Society, 2012, Berlin, Germany.*

[13] **Weiss, M.**, **Esfandiari, B.** and **Luo, Y.**, Towards a Classification of Web Service Feature Interactions, *Computer Networks* **51**(2):359-381 (2007).

[14] **Weiss, M.** and **Esfandiari, B.**, On Feature Interactions among Web Services, *Proc. IEEE Int. Conf. on Web Services, 2004, San Diego, California, USA,* pp. 88–95.

[15] **Bond, G.**, **Cheung, E.**, **Fikouras, I.** and **Levenshteyn, R.**, Unified Telecom and Web Services Composition: Problem Definition and Future Directions, *Proc. IPTCOMM, 2004, Atlanta, USA.*

[16] **Kolberg, M.** and **Magill, E.**, Detecting Feature Interactions between SIP Call Control Services, *Proc. Feature interactions in telecom. and software systems VIII, 2005, Leicester, UK.*

[17] **Chentouf, Z.**, **Cherkaoui, S.** and **Khoumsi, A.**, Service Interaction Management in SIP User Device Using Feature Interaction Management Language, *Proc. NOuvelles TEchnologies de la RÉpartition (NOTERE), 2004, Saïdia, Morocco.*

[18] **Xu, J.**, **Yu, W.**, **Chen, K.** and **Reiff-Marganiec, S.**, Web Services Feature Interaction Detection based on Situation Calculus. *Proc. IEEE World Congress on Services, 2010, Miami, Florida, USA,* pp. 213-220.

[19] **Zhao, Q., Huang, G.** and **Mei, H.**, An On-the-fly Approach to Web-based Service Composition, *Proc. IEEE Congress on Services Part II, 2008, Beijing, China,* pp. 208-209.
[20] **Zhao, Q.** and **Huang, J.**, Feature Interaction Problems in Web-based Service Composition, *Proc. Int. Conf. on feature Interactions (ICFI), 2009, Lisbon, Portugal,* pp. 234-241.
[21] **Weiss, M.** and **Esfandiari, B.**, Offline Detection of Functional Feature Interactions of Web Services, *Proc. Montreal Conf. on eTechnologies (MCeTech), 2006, Montreal, Canada,* pp. 129-136.
[22] **Zhang, J., Su, S.** and **Yang, F.**, Detecting Race Conditions in Web Services, *Proc. Advanced International Conf. on Telecommunications and Int. Conf. on Internet and Web Applications and Services (AICT/ICIW), 2006, Guadeloupe, French Caribbean.*
[23] **Thomas, J.P.** and **Ghinea, G.**, Modeling of Web Services, *Proc. Int. Conf. on E-Commerce (CEC),2003, Newport Beach, California, USA.*
[24] **Luo, X.** and **Dong, R.**, Detecting Feature Interactions in Web Services with Timed Automata. *Proc. Int. Conf. on Genetic and Evolutionary Computing (WGEC), 2009, Guilin, China*, pp. 276-279.
[25] **Zhang, J., Yang, F.** and **Su, S.,** Detecting Feature Interactions in Web Services with Model Checking Techniques, *The Journal of China Universities of Posts and Telecom.* **14**(30):108-112 (2007).
[26] **Holzmann, G.J.,** The Model Checker SPIN, *IEEE Trans. on Software Eng.* **23**(5):279-295 (1997).
[27] **Andrews, T.**, Business Process Execution Language for Web Services, Version 1.1, Retrieved: April 1, 2011, from http://www-106.ibm.com/developerworks/library/ws-bpel/ (2003).
[28] **Liu, X., Hui, Y., Sun, W.** and **Liang, H.,** Towards Service Composition Based on Mashup, *Proc. of IEEE Congress on Services, 2007, Salt Lake City, Utah, USA.*
[29] **Chafle, X.**, An Integrated Development Environment for Web Service Composition, *Proc. IEEE Int. Conf. on Web Services (ICWS), 2007, Salt Lake City, Utah, USA.*
[30] **Karunamurthy, R.** and **Khendek, F.**, A Novel Business Model for Web Service Composition, *Proc. IEEE Int. Conf. on Services Computing (SCC), 2006, Chicago, Illinois, USA.*
[31] **Karunamurthy, R., Khendek, F.** and **Glitho, R.,** A Business Model for Dynamic Composition of Telecom. Web Services, *IEEE Communications Magazine* **22**(3): 154-169 (2007).
[32] **Booth, D.**, Web Services Architecture, W3C Working Group Note, Retrieved April 1, 2011 from http://www.w3.org/TR/ws-arch/ (2004).
[33] **Karunamurthy, R., Khendek, F.** and **Glitho, R.**, Categorizing and Assembling Web Services in a Composition Framework, *Proc. IEEE Software Engineering Workshop, 2009, Skövde, Sweden.*
[34] **Turner, K.J.**, Formalising Web Services. *In Proc. Formal Techniques for Networked and Distributed Systems (FORTE XVIII), 2005, Taipei, Taiwan.*
[35] **Turner, K.J.**, Representing and Analyzing Composed Web Services using CRESS, *Network and Computer Applications* **30**(2):541-562 (2007).
[36] **Liu, A.X.** and **Gouda, M.G.**, Diverse Firewall Design, *IEEE Trans. on Parallel and Distributed Systems* **19**(8):1-15 (2008).

استخدام وتعديل إطار عمل لكشف التفاعلات ذات الخصوصية في خدمات الويب

أحمد خمسي، وزهير شنتوف*

قسم الإلكترونيات وهندسة الحاسبات، جامعة شيربروك، شيربروك، كندا، و قسم هندسة البرمجيات، كلية المعلومات وعلوم الحاسبات، جامعة الملك سعود، الرياض، المملكة العربية السعودية*

zchentouf@ksu.edu.sa

المستخلص. إحدى فوائد تركيب خدمات الويب هي الحصول على خدمات جديدة من خدمات موجودة مسبقًا. ولكن تركيب خدمات الويب قد تكون عرضة لبعض التفاعلات الخاصة والتي تؤدي إلى حدوث تصرفات غير مرغوب فيها عند استخدام أكثر من خدمة ويب مع بعضها البعض. ولقد أضحى معروفًا اليوم أن طرائق اكتشاف التفاعلات ذات الخصوصية تفضي إلى تعقيد يصعب التحكم فيه دون أن يضعف ذلك من قدرتها على اكتشاف الأخطاء. هدف البحث هو تطوير طريقة لاكتشاف التفاعلات الخاصة في خدمات الويب والتي تهدف إلى تقليل التعقيدات التي يصعب التحكم فيها، بينما نحاول الحفاظ على قدر مقبول من اكتشاف التفاعلات ذات الخصوصية. الطريقة المقترحة تعتمد على استخدام لغة جديدة لنمذجة خدمات الويب بمستوى تجريدي عالي. يقدم نموذج الاستخدام والتعديل لخدمات الويب معلومات مثل "من يستخدم ماذا" و"من يعدل ماذا" ويميز كل عملية استخدام وتعديل بـ "دائمًا" و"أحيانًا" و"أبدًا" و"ربما". الاستخدام والتعديل يشيران أيضًا إلى كل استخدام وتعديل إذا كانت شروطًا محددة أو غير محددة. درسنا التعقيد الحسابي لطريقتنا لكشف التفاعلات ذات الخصوصية ووضحنا قابليتها للتطبيق في عدة أمثلة.

JKAU: Comp. IT., **Vol. 3**, pp: 51 - 69 (2014 A.D./ 1436 A.H.)

DOI: 10.4197 / Comp. 3 -1.2

Feasibility Verification and Performance Evaluation of Exclusion-Based VANETs (EBV)

Ahmad A. Al-Daraiseh, Mohammed A. Moharrum*, and **Ahmed Youssef**

*Department of Information Systems, King Saud University, and *Deanship of Scientific Research, Al Imam Muhammed Ibn Saud Islamic University, Riyadh, Saudi Arabia*

adaraiseh@ksu.edu.sa

Abstract. Vehicular Ad-hoc NETworks (VANETs) are wireless networks that help improve driving efficiency and safety. VANETs provide a wide range of road services such as detecting traffic congestion, finding alternative routes, estimating time to destination, collision warning and many others. One of the biggest challenges in deploying VANETs is how to successfully address their security issues. These issues are mainly due to conflicting security requirements such as privacy and linkability. Exclusion-Based VANETs (EBV) was proposed as a generic framework to resolve some of VANETs' security issues. In this paper, we verify the feasibility and evaluate the performance of EBV through a set of simulation experiments. We measure time taken to deliver messages, packet loss, and average throughput. The results showed that EBV is competitive to other protocols in terms of efficiency and cost.

Keywords: VANETs, Exclusion-Based System (EBS), Security, PKI.

1. Introduction

Vehicular Ad-hoc NETworks (VANETs) are special version of Mobile Ad hoc Networks (MANETs) used within vehicles as well as other facilities to improve traffic management. In VANETs, each vehicle is equipped with a wireless On-Board Unit (OBU) that allows the vehicle to communicate with other vehicles or with Road Side Units (RSUs) through short range wireless communication. VANETs communication may be classified as either vehicle to vehicle (V-V) or vehicle to infrastructure (V-I) communication. Several types of VANETs applications have been proposed in the literature. Examples of these applications are safety[1], entertainment[2], and information sharing applications[3]. A recent comprehensive survey on VANETs can be found in [10, 38, 41].

Securing VANETs implies different requirements including message integrity and authentication, vehicle privacy and confidentiality, non-repudiation, and short term linkability for investigation purposes. In addition, most applications, especially safety applications, require almost real-time message processing to satisfy application requirements. Providing security to VANETs applications is a very challenging task that has been widely explored in the last decade. The challenge lies in how to satisfy conflicting security requirements such as privacy on one side and linkability on the other side. Mobility with limited processing capabilities of installed hardware is another issue that needs to be addressed.

Key management is a main issue in securing VANETs. Despite the fact that Public key Infrastructure (PKI) is very successful in many applications, we believe that PKI alone might not be able to fulfill all the security requirements exist in VANETs under different conditions. Consider, for example, a transmission range of 150 m (i.e. 300 diameters) and heartbeat message frequency of 10Hz, as suggested in [4]. Under these conditions, number of messages, Certificate Revocation List (CRL) size, and the hardware limitations represent major obstacles that render developing a secure architecture for VANETs application a dilemma.

In our previous work[5], we proposed Exclusion-Based VANETs (EBV), a generic framework for VANETs that uses a combination of PKI and symmetric key management to resolve some VANETs security issues. In this paper, we verify the feasibility of EBV and evaluate its performance through a set of simulation experiments. We've taken measure time to deliver messages, packet loss, and average throughput.

The rest of this paper is organized as follows: in section 2, we present some related work. In section 3, we review EBV structure and operations. In section 4, we evaluate EBV performance through a set of simulation experiments and report our results. Finally, in section 5, we give our conclusions and future work.

2. Related Work

The Elliptic Curve Digital Signature Algorithm (ECDSA) for signatures is used in the current IEEE 1609.2 standard for secure VANETs communications to verify messages[2]. Prior work has shown that the verification of single ECDSA signature requires 7ms of computation on proposed On Board Unit (OBU) hardware[8]. An efficient alternative to signatures is TESLA authentication technique[6]. In TESLA, symmetric cryptography with delayed key disclosure is used to provide the necessary asymmetry to prove that the sender was the source of the message. However, TESLA suffers from vulnerability to memory-based DoS attacks. A hybrid authentication mechanism was proposed in[7] which combines VANETs authentication using ECDSA signatures and TESLA++ (VAST) and provides the advantages of both of them.

Many solutions have been suggested to address the security issues in VANETs. The authors in[10] classified VANET security schemes into PKI-based schemes and non PKI-based schemes. They provided a comparison between the two different schemes in terms of efficiency, scalability, authenticity, integrity, short term linkability, privacy and non-repudiation. In[9] the authors identified two categories of VANETs security solutions: PKI and the ID-Public Key Cryptosystem (ID-PKC). In PKI solutions, group signature is used as a cryptographic basis to achieve security requirements. For efficiency and scalability reasons, PKI based systems are combined with other cryptographic based systems, such as ID based cryptography. In the following two sub-sections, we review the previous work in the two categories and determine how each category meets the security requirements.

2.1 PKI proposals

There have been several proposals for achieving security requirements in VANETs based on PKI. There are early schemes[11] and[12] and more advanced schemes which may be classified as either with pseudonyms [13-16] or group signature [9, 17-20]. Pseudonyms have been used to protect the real identity of the vehicles. Using pseudonyms requires vehicles to store a large number of pseudonyms and certificates, where it is not convenient to implement a revocation scheme to revoke the malicious vehicle. Moreover, the pure pseudonym schemes do not support the secure functionality of authentication, integrity, and non-repudiation.

Traditional digital signature scheme, where a vehicle stores a very large number of public/private key pairs; has been proposed in[20] to address the privacy issue in VANETs. To achieve both message authentication and anonymity, the authors[20] proposed that each vehicle should be preloaded with a large number of anonymous public and private key pairs and the corresponding public key certificates. The authors in[21] introduced a group signature scheme to sign each message. In this scheme, each vehicle has its own private key and all group members share one public key. The work in[22] combines pseudonym schemes with group signature to avoid storing pseudonyms and certificates in vehicles.

Although the work described above provides strong security features such as authentication, non-repudiation, and confidentiality, they are not likely to be widely available because they require extra communication for the maintenance of public key certificates and for the management of CRLs. For these critical drawbacks, researchers investigated the use of other cryptographic schemes to be combined with PKI-based solutions.

2.2 ID-PKC proposals

ID-Public Key Cryptosystem (ID-PKC) [7] have been introduced in[9, 23-25]. In such cryptosystem, the user's information, such as phone number and e-mail address, can be used as a public key for verification and encryption. In other words, the ID-based cryptosystem simplifies the certificate management process. Kamat *et al*[23] proposed an ID-based security framework for VANETs. They use the ID-based signcryption scheme to provide authentication, confidentiality, message integrity, nonrepudiation and pseudonymity. In[26] the authors discussed approaches to prevent vehicles from fabricating their position information. Sun *et al*[25] presented a security framework that assures privacy using the preloading pseudonym and non-repudiation through an ID-based threshold signature scheme. Lin *et al*[9] proposed the RSU-aided certificate revocation scheme. In[24], the authors proposed SECSPP, a secure and efficient communication scheme based on non-interactive ID-based public-key cryptography, blind signature, and one-way hash chain.

Unfortunately, in all previous security frameworks, the private/public keys of VANET nodes are assigned by the Key Generation Center (KGC), which causes inherent weaknesses such as key escrow. The key escrow problem implies that: since the KGC issues their private keys using the master key, it may decrypt or sign any message[37]. This cannot guarantee strong non-repudiation and private communication because the KGC can sign and decrypt any message and abuse its accessibility. In[27], Zhang, *et al.*, proposed RAISE in which Vehicles generate a shared symmetric key with the RSU using a Diffie-Hellman key agreement protocol. RSUs then become responsible for verifying the authenticity of the messages sent by vehicles. RAISE addressed the issue of VANETs scalability and communication overhead in case of large traffic intensity.

In[28] the authors proposed a security architecture to handle key escrow, in which a vehicle updates its private and public keys, and sends them to Road Traffic Utility (RTA) to be verified. The RTA generates the vehicle's new signature and sends it back. In[29], the authors propose the use of certificate-based cryptography as a hybrid approach to combine the advantages of ID-based cryptography as well as the PKI approach. Several proposals were introduced on secure beaconing. In[30], the authors proposed the usage of radar device attached to the front and the back of the vehicle in addition to a GPS receiver. In[10], the authors studied existing security protocols, and they concluded that a main drawback is the lack of practical feasibility because of network overhead.

Recently, S. Junggab *et al*[39] introduced the first VANET cloud architecture. They also, identified the unique security issues and challenges when utilizing the cloud. A. Nikolaos *et al*[40] utilized tickets as cryptographic tokens to comply with vehicular communication standards yet preserve the privacy of the vehicle. D. Kevin *et al*[42] proposed the use of a tree like structure and called multi-level security architecture for VANETs. In this work when a node is attacked the parent node will deactivate the attacked node and redistribute the keys in that area.

3. EBV Structure and Operation

EBV[5] is a novel framework that utilizes Exclusion-Based System (EBS)[31-33], Advanced Encryption Standard (AES) and PKI to create a robust, efficient, and scalable security solution for VANETs. In our previous work EBV [5], we utilized Exclusion Based System EBS , which was originally developed and tested for both security and efficiency in[31]. It was used further as a basis for several ad-hoc and sensor network key management in several papers, examples include[32, 33].

Our proposed EBV consists of the following hierarchically organized entities (Fig. 1.):

- **Global VANET Authority (GVA):** a trusted party that registers and manages CVAs, run by an international cooperation.
- **Country VANET Authority (CVA):** trusted country wide authority that registers all country's RVAs, run by national DMV.
- **Regional VANET Authority (RVA):** a trusted regional authority that manages an EBS system in a specific region (could be a city or a state), run by regional DMV.
- **Road Side Unit (RSU):** a node in VANETs that relays messages between vehicles and RVAs and vice versa.
- **Vehicles:** normal vehicles and special ones (e.g., Police and emergency vehicles).

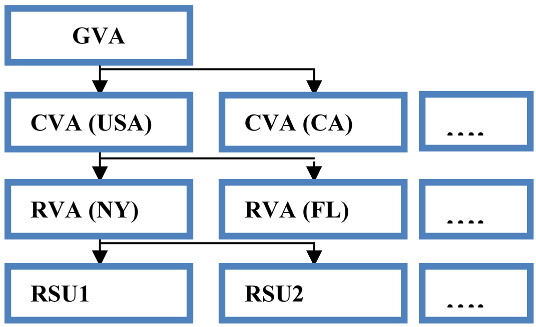


Fig. 1. EBV structure.

EBV framework resists several types of attacks including bogus information, unauthorized preemption, message replay and modification, impersonation, RSU relocation, movement tracking, impersonating an RSU, malicious vehicle, brute force, and illusion attacks[5]. The operation of EBV has three main phases which are described below.

3.1 Initialization and Registration Phase

When an RVA is deployed, it calculates a canonical matrix A[k+m, C(k+m,k)] with a large number of columns (i.e. larger than the number of vehicles expected in this region in the next 100 years). When choosing integers k and m an RVA preserves the following:

- The number of keys (*i.e.* k + m) is kept small. 58 (8 + 50) was used in the simulation generating a reasonable matrix of around 2 billion entries.
- m should be large enough (*i.e.* the number of vehicles an attacker needs

to attack to reveal all keys of the group should be very large).

RVA initially loads every vehicle and RSU with the following items:

- 10-Digit vehicle identifier (VID, RSUID in case of RSU) allows for 10 billion different vehicles/RSUs.
- KGF a one-way trapdoor Key Generation Function. MD5 was used.
- 128bit session key S_n, the current key in this area and its sequence number (SKSN 2Byte).
- A set of 8 administrative keys 128bit each generated by RVA. RVA maps every vehicle ID to a column in the matrix A, as well as, to the real identity of the vehicle.
- A bit string (BSV) of 58 bits that represents the column from matrix A assigned to this specific vehicle V, where a 1 means the vehicle has the key.
- RVA's Public key (RVA_e) and Product value N. (RSA 1024bit is used)
- Previous session key's sequence number.
- Previous key update message.

3.2 Normal Operation Phase

In EBV, the following events could occur in normal operation phase:

a) B_{msg} Exchange

Every vehicle and RSU use the current session key (S_n) to securely communicate beacons. The proposed message format is shown in Fig. 2.

8B	2B	8B	8B	2B	0.5B	21.5B
TS	SKSN	X pos	Y pos	Speed	Direction	Application Specific Info

Fig. 2. Proposed 50byte message format.

To provide a B_{msg} with integrity, authenticity, non-repudiation, and linkability by RVA, a message (MSG) is attached to a signature-like string before sending it as follows:

Get a 16B hash of MSG using MD5 function:

$$MSG_{Hash} = MD5\ (MSG) \tag{1}$$

Get a 16B hash of all eight admin keys, ($K_1,\ldots,K_8$), concatenated:

$$K_{Hash} = MD5\ (K_1|K_2|\ K_3|K_4|K_5|K_6|K_7|K_8) \tag{2}$$

XOR MSG_{Hash} and K_{Hash}:

$$XOR_{Hash} = MSG_{Hash} \wedge K_{Hash} \tag{3}$$

Append vehicle ID (VID) to XOR_{Hash}:

$$plainSig = XOR_{Hash}\ |\ VID \tag{4}$$

Use RVA's public key RVA_e to RSA encrypt plainSig:

$$SIG = RSA_{RVAe}\ (plainSig) \tag{5}$$

Use AES and Sn to encrypt MSG as follows:

$$encMSG = AES\_ENC_{Sn}\ (MSG) \tag{6}$$

A vehicle creates a heartbeat message (B_{msg}) by concatenating a Time Stamp (TS), a Sequence Number of the current session key SKSN, encMSG and SIG, as follows:

$$B_{msg} = TS \mid SKSN \mid encMSG \mid SIG \tag{7}$$

Upon receiving a B_{msg}, a vehicle checks TS, if within application's acceptable limits, it checks to see if SKSN is current. If correct, it uses its session key S_n to decrypt the message.

$$PlainMsg = AES\_DEC_{Sn}\ (encMSG) \tag{8}$$

If the decrypted TS and SKSN match the plain ones, it means an owner of S_n only could have generated the message. It then forwards the data to the installed application/s. The signature SIG will be ignored by receiving vehicles.

b) Updating session key

The session key, S_n, is changed regularly to prevent statistical attacks. The new key S_{n+1} will be sent out through RSUs to all vehicles encrypted as follows:

$$AES\_ENC_{Sn}\ (S_{n+1}) \mid RVA_{Signature} \mid RVA_{certificate} \tag{9}$$

Where RVA signature and certificate are standard RSA's. A receiving vehicle would use RVA's (e,N) to verify the attached signature. If valid, a vehicle would use AES_DEC_{sn} to decrypt the new session key S_{n+1} and increment SKSN, otherwise it would ignore the message. If used, the message will be stored until the next update occurs.

c) Key request

If a vehicle V has been away from the network for long time, it might miss more than one key update message. It will realize this when receiving at least 10 B_{msg} from different vehicles where:

$$SKSN\ of\ B_{msg} <> (V's\ SKSN)\ \&\&\ SKSN\ of\ B_{msg} <> (V's\ SKSN +1)\ Mod\ 65535 \tag{10}$$

V will stop sending B_{msg}s to save bandwidth (BW). As soon as V receives a B_{msg} from an RSU, it will send a Request for Key message (RK_{msg}). In a Diffie–Hellman like style, it creates an RSA public V_e, private V_d key pair, a product V_n and a random request identifier RID (these are created offline to save time), then, it uses RVA's (e,N) to encrypt the message as follows:

$$R_{msg} = RSA_{RVAe}(VID \mid RID \mid VS_n \mid V_e \mid V_n) \tag{11}$$

Where VS_n is the session key of V.

$$R_{hash} = MD5(R_{msg} \mid K_1|K_2\ldots|K_k) \tag{12}$$

$$RK_{msg} = R_{msg} \mid R_{hash} \tag{13}$$

The message is broadcasted and then forwarded by the RSU to the RVA. RVA uses its private key RVA_d to verify the message as follows:

$$plainMsg = RSA_{RVAd}(R_{msg}) \tag{14}$$

Based on VID and VS_n, it gets the k keys of the vehicle that existed when Vs was in use from a key repository it has (remember that some of the k keys might have been modified when the vehicle was away). Then, it regenerates the signature R_{hash} using the keys it retrieved from the matrix as follows:

$$R_{hash1} = MD5(R_{msg} \mid K_1 | K_2 \ldots | K_m) \tag{15}$$

If $R_{hash1} = R_{hash}$, then the vehicle is authentic. Otherwise RVA ignores the message. If authentic and VID was not revoked, RVA creates a reply message RRK_{msg} and sends it to the RSU that forwarded RK_{msg} as follows:

$$encRK_{msg} = RSA_{Ve}(S_n \mid SKSN \mid K_1' | \ldots . | K_m') \tag{16}$$

$$RRK_{msg} = RID \mid encRK_{msg} \mid RVA_{Signature} \mid RVA_{certificate} \tag{17}$$

Where S_n and SKSN are the current session key and its sequence number, and (K_1'|….| K_m') are V's current admin keys. The originator RSU will broadcast RRK_{msg}. If received by the requesting vehicle that checks RID to make sure this reply is intended to it, it then uses RVA's (e,N) to verify the attached signature and uses V_d to decrypt the message

$$plainMsg = RSA_{Vd} (encRK_{msg}) \tag{18}$$

It then updates the keys where it has by replacing the old ones with the new ones.

d) Rekey process

RVA may decide that a certain vehicle needs to be evicted which based on a strong evidence where it has (getting the evidence is outside the scope of this paper). RVA starts a rekey process in the region, where all keys are known to the evicted vehicle X that will be modified by every other vehicle. Table1 shows a possible distribution of X's eight keys K_{e1} to K_{e8} and its bit-string BSX as stored in RVA to make things clearer.

The process starts by RVA issuing a new session key S_{n+1} and eight admin keys to replace the keys into vehicle X that knows. *i.e.* K_{e1} through K_{e8}. The other m = 50 keys, K_1 through K_m Stay the same.

Table 1. A possible distribution of vehicle X's k keys along with its bit-string as stored in RVA.

K_{index}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
K or Ke	K1	K2	K3	K4	K5	Ke1	K6	K7	K8	K9	Ke2	K10	K11	K12	K13
BSX	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0
K_{index}	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
K or Ke	K14	K15	K16	Ke3	K17	K18	K19	K20	Ke4	K21	K22	K23	K24	K25	K26
BSX	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0
K_{index}	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
K or Ke	K27	K28	Ke5	K29	K30	K31	K32	K33	K34	K35	K36	K37	K38	Ke6	K39
BSX	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
K_{index}	46	47	48	49	50	51	52	53	54	55	56	57	58		
K or Ke	K40	K41	K42	K43	Ke7	K44	K45	K46	K47	K48	K49	Ke8	K50		
BSX	0	0	0	0	1	0	0	0	0	0	0	1	0		

RVA generates replacement keys by repeating the following operation k times once for each key:

$$K_{ei} = MD5\ (S_{n+1} \mid K_{ei}) \tag{19}$$

RVA broadcasts the Rekey message, by broadcasting X's bit-string (BSX) in a message composed of the following m parts:

$$Part_i = K_{index} \mid AES\_ENC_{Ki}\ (S_{n+1}) \tag{20}$$

where 1<= i <=m=50, and K_{index} is the absolute index of K_i as shown in Table1. In this $Part_i$ we are sending the new session key S_{n+1} encrypted using one of the m keys (K_i) which vehicle X doesn't have. We are attaching the absolute index of the key K_i to make it easier for receiving vehicles to know which key to use to decrypt this part.

After generating 50 Parts, the message $ReKey_{msg}$:

$$ReKey_{msg} = AES\_ENC_{Sn}(BSX \mid Part_1 \mid Part_2 \mid .... \mid Part_m) \mid RVA_{signature} \mid RVA_{certificate} \tag{21}$$

Upon receiving the message, Each RSU broadcasts the message on behalf of the RVA.

After verifying a received message, a vehicle uses S_n to decrypt the first level of encryption and extract BSX and m Parts:

$$plainMsg = AES\_DEC_{Sn}\ (M) \tag{22}$$

Where M = $AES\_ENC_{Sn}(BSX \mid Part_1 \mid Part_2 \mid .... \mid Part_m)$.

A vehicle checks BSX to see if it shares any keys with the evicted vehicle. If so, it continues to decrypt the jth Part with K_j, any of its k keys:

$$plainPart_j = AES\_DEC_{Kj}(Part_j) \quad (23)$$

Once it decrypts any of the m Parts, it updates its session key S_n and uses it to replace all the keys it shares with vehicle X according BSX, by executing operations similar to (19). Every vehicle should store the rekey message it receives until the next eviction or periodic change of S_n occurs.

e) Forwarding key update message:

If a vehicle A that has a current session key S_n is met with another vehicle B that uses the previous session key S_{n-1}, all A has to do is to replay the stored session key or Rekey message it stores. If the vehicle B possess S_{n-1} and is not revoked, it should be able to update its keys as described in updating a session key or in the rekey sections above.

3.3 Crossing Boarders Phase

When a vehicle from region R_1 approaches another region R_2, it follows a procedure identical to that of a Key Request described above. The receiving RSU in R_2 relays the message to its RVA (i.e., RVA_2) that manages R2. RVA_2 sends the message to RVA_1 to make sure that the vehicle is not revoked and if so to get the message's plain text (only RVA_1 knows how to decrypt the message). Upon receiving the reply from RVA_1, RVA_2 checks to see if this vehicle has a record in its matrix. If not, it registers the vehicle then it uses an identical technique to respond to the vehicle as described above. Otherwise, a reply message is directly constructed and sent. This phase was not simulated due to limitations in the software packages used and was left for future work.

4. Simulation Results

To our knowledge, EBV is the first utilization of EBS in VANETs, and hence, comparison with other models in many aspects was not an option. To verify EBV's feasibility, we decided to start by a simple simulation that uses one straight highway with one entrance and one exit. In our simulation we used NS3 in conjunction with VANET-Highway Package (VHP)[34]. VHP utilizes NS3 and provides traffic simulation capabilities; so that no external traffic traces are needed. In the following sub-sections, we explain the simulation parameters we used and report the simulation results.

4.1 Simulation Parameters

To carry out the simulation of EBV, we had to modify the following classes from the VHP: Controller, Highway, and Vehicle class.

These classes were modified to support EBV encryption and decryption. We also created the following new classes:

- AESEncryption: a class used to allow symmetric encryption/decryption.
- MDHashing: a class that implements MD5 hashing.
- RSAEncrDecr: a class used to allow RSA encryption/decryption.
- RoadSideUnit: a class that works as an RSU in an EBV system.
- RvaEbs: a class that works as an RVA in an EBV system.

All experiments were carried out on a Dell Latitude laptop with 2.53 GHz Core 2 Duo CPU and 4GB RAM. Simulation parameters were as follows:

- Highway: One-way, three lanes, 2.4 Km in length.
- RSUs: Three RSUs located at 400m, 1200m and 2000m. RSU_1 acts as an RVA to the system.
- Vehicles: 80% sedan, 20% truck, all equipped with wi-fi devices 250 - 400 m range, speed up to 29m/s.
- Traffic flow and gap between vehicles : variable
- RVA: updates session key every 15s and randomly revokes a vehicle every 27s.
- B_{msg} frequency: every 0.1 – 0.3s random.
- Encryption/decryption: 128bit symmetric and 1024bit RSA.
- Simulation time: 300s

The simulation was repeated 300 times and an average of each measured value was considered.

4.2 Simulation Results

The results of our simulation were very promising. In our first experiment, we measured the time it takes a vehicle to do each of the following actions:

- Encrypt/decrypt a B_{msg}.
- Create/verify a B_{msg} signature.
- Create/extract Keyupdate message.

The results are shown in Table 2 below.

Table 2. EBV TIME MEASUREMENTS.

	Bmsg		**Bmsg Sig**		**Keyupdate message**	
	Encrypt	***Decrypt***	***Create***	***Verify***	***Create***	***Verify***
Time ms	0.125	0.27	0.075	3.18	8	0.55

It is very obvious that the time needed to do all operations in the OBU is quite small. In fact an OBU needs to receive from 740 vehicles sending 5 B_{msg}/s to stay busy all the time. It was reported in[35] that signing/verification using 1024-RSA onboard requires 52/0.8ms, it is clear that our technique is well below in signing and slightly higher in verifying. On a similar hardware J. Hass[6] reported that signing/verification of ECDSA took around 1.5/1.8ms and for TESLA around 10µs to verify. Notice that the largest two measurements (3.18 and 8 ms) are done only by an RVA. We believe that OBU hardware should be at least equal to that we are using in these experiments.

To make sure that a key update message is distributed within a reasonable time, we performed our second experiment. We monitored all vehicles on the road after sending such message and recorded the average time it takes until all vehicles on the road are updated with new keys. We did this with different traffic intensities on the road and the results are shown in Fig. 3.

Fig. 3 shows that the maximum time to deliver keys to all vehicles on the road was around 0.25s, and the minimum was 0.1s. It is interesting to see that the time was higher at lower vehicle intensity. We believe that this was due to the forwarding mechanism we implemented. The higher the number of vehicles on the road gives more chance for this mechanism to be utilized. It was reported in[36] that the time required to distribute a CRL to 175 vehicles with best used technique was more than 25s. It is obvious that EBV revokes a vehicle in less than 0.5s. Also[6] reported that distributing a CRL to all vehicles in his simulation took well over 1000s with the best used technique.

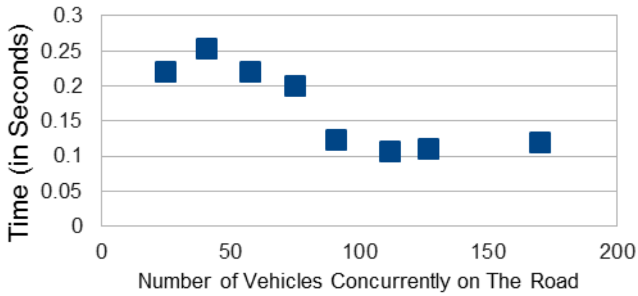


Fig. 3. Time to Deliver Key updates Messages.

In the third experiment, we try to make sure that sending Bmsgs at such a high rate regardless of vehicle intensity does not consume too much bandwidth (BW). We measured the used BW for different vehicle intensities and the results are shown in Fig. 4. The results were as expected and the BW used increased almost linearly as the number of vehicles increased. The BW maxed out at less than 3Mbps when the number of vehicles was a little more than 170.

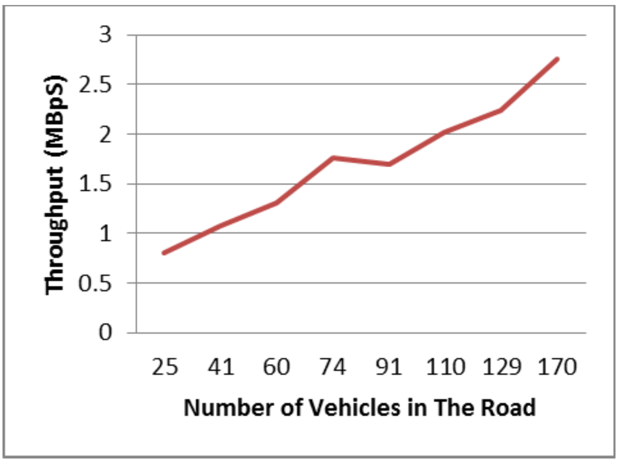


Fig. 4. Average Throughput Change with the Number of Co-existing Vehicles

To check the effect of traffic intensity on loss ratio, we performed our fourth experiment. We measured the loss ratio at different traffic intensities. Fig. 5 shows that when the number of vehicles was 25 a loss ratio was around 4% and when the number of vehicles was 175, the loss was less than 6%. Although we don't have much in common with[25], our traffic intensities are very close. A comparison between our results and a reconstructed curve from [25] shows that our system tends to have higher values for low intensities but for higher intensities our system gives better results.

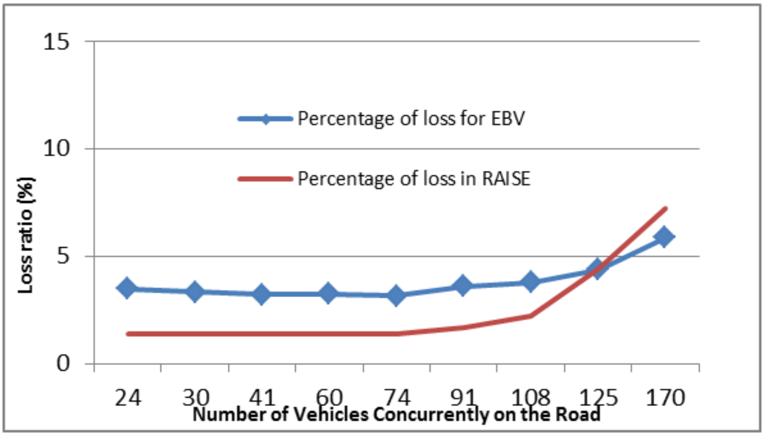


Fig. 5. Packet loss ratio vs traffic intensity.

Time and space complexities are not discussed in this paper because it only deals with simulating EBV and the simulation results. The readers are advised to check the works at[5, 31-33] for algorithmic analysis.

5. Conclusions

Key and CRL management in VANETs is a very difficult and time consuming task. While many proposed frameworks for VANETs achieve security, we believe they will not be adopted because of suffering any or a combination of: Certificate revocation list management, large computation time, large communication overhead, lack of scalability, or inability to defend some of the attacks.

In this paper, we tried to verify the feasibility of EBV (previously proposed by the authors) and study its efficiency through simulation using NS3. Our simulation experiments studied delivery time, throughput, and packet loss ratio under different numbers of vehicles and distances. Although a comparison to other protocols was very hard to do because of the different architecture and simulation tools and scenarios, our results shows competitiveness of EBV to other existing protocols considering both computation cost and efficiency.

We believe that our framework needs a full scale simulation, which considers real/artificial road maps with real/artificial traffic traces to be able to compare to other existing solutions. Another future work issue is to utilize DSRC instead of wi-fi as it has been set as a standard.

References

[1] **C. L. Robinson, L. Caminiti, D. Caveney,** and **K. Laberteaux**, "Efficient coordination and transmission of data for cooperative vehicular safety applications," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks* Los Angeles, CA, USA: ACM, 2006.

[2] **C. E. Palazzi**, "Fast Online Gaming over Wireless Networks." vol. Doctor of Philosophy in Computer Science Los Angeles: University of California, 2007.

[3] **T. Kitani, T. Shinkawa, N. Shibata, K. Yasumoto, M. Ito,** and **T. Higashino**, "Efficient VANET-Based Traffic Information Sharing using Buses on Regular Routes," in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, 2008, pp. 3031-3036.

[4] **V. S. Communications**, "Vehicle safety communications project-final report," 2006.

[5] **A. A. Al-Daraiseh and M. A. Moharrum**, "Exclusion Based VANETs (EBV)," in *Secure and Trust Computing, Data Management and Applications*. vol. 186: Springer Berlin Heidelberg, 2011, pp. 96-104.

[6] **J. J. Haas, H. Yih-Chun,** and **K. P. Laberteaux**, "Real-World VANET Security Protocol Performance," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 2009, pp. 1-7.

[7] **A. Studer, F. Bai, B. Bellur,** and **A. Perrig**, "Flexible, Extensible, and Efficient VANET authentication," in *in 6th Conference on Embedded Security in Cars (Escar)* Hamburg, Germany, March 2008, p. 22.

[8] **R. Maxim** and **H. Jean-Pierre**, "The Security of Vehicular ad hoc Networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks* Alexandria, VA, , 2005, pp. Pages: 11 - 21.

[9] **L. Xiaodong, L. Rongxing, Z. Chenxi, Z. Haojin, H. Pin-Han,** and **S. Xuemin**, "Security in vehicular ad hoc networks," *IEEE Communications Magazine,* vol. 46, pp. 88-95, Feb. 2008.

[10] **M. A. Moharrum** and **A. Al-Daraiseh**, "Toward Secure VANETs: A Survey," *IETE Technical Review", vol. 29,* Issue 1, pp.80-89, 2012.

[11] **K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura,** and **K. Sezaki**, "CARAVAN: Providing Location Privacy for VANET," in *3rd International Workshop on Vehicular ad hoc Networks,* Cologne, September 2006.

[12] **S. Amit Kumar** and **B. J. David**, "Modeling mobility for vehicular ad-hoc networks," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks* Philadelphia, PA, October 2004.

[13] **A. R. Beresford** and **F. Stajano**, "Mix zones: user privacy in location-aware services," in *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, 2004, pp. 127-131.

[14] **M. Gerlach** and **F. Guttler**, "Privacy in VANETs using Changing Pseudonyms - Ideal and Real," in *IEEE 65th Vehicular Technology Conference, VTC*, Dublin April 2007, pp. 2521-2525.

[15] **G. Philippe, G. Dan,** and **S. Jessica**, "Detecting and correcting malicious data in VANETs," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks* Philadelphia, PA, USA: ACM, 2004.

[16] **M. Raya, P. Papadimitratos,** and **J. P. Hubaux**, "Securing Vehicular Communications," *IEEE Wireless Communications, ,* vol. 13, pp. 8-15, October 2006

[17] **M. Franklin, D. Boneh, X. Boyen,** and **H. Shacham**, "Short Group Signatures," in *Advances in Cryptology – CRYPTO 2004*. vol. 3152: Springer Berlin / Heidelberg, 2004, pp. 227-242.
[18] **G. Jinhua, J. P. Baugh,** and **W. Shengquan**, "A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework," in *Mobile Networking for Vehicular Environments*, Anchorage, ALASKA,, May 2007, pp. 103-108.
[19] **H. Leping, K. Matsuura, H. Yamane,** and **K. Sezaki**, "Enhancing wireless location privacy using silent period," in *IEEE Wireless Communications and Networking Conference,* , Nokia Res. Center Japan, Tokyo, Japan May 2005, pp: 1187-1192.
[20] **M. Raya** and **J.-P. Hubaux**, "Securing vehicular ad hoc networks," *Journal of Computer Security,* vol. 15, pp: 39-68, 2007.
[21] **L. Xiaodong, S. Xiaoting, H. Pin-Han,** and **S. Xuemin**, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," *IEEE Transactions on Vehicular Technology, ,* vol. 56, pp: 3442-3456, November 2007.
[22] **C. Giorgio, P. Panos, H. Jean-Pierre,** and **L. Antonio**, "Efficient and robust pseudonymous authentication in VANET," in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks* Montreal, Quebec, Canada: ACM, 2007.
[23] **K. Pandurang, B. Arati,** and **T. Wade**, "An identity-based security framework For VANETs," in *The Proceedings of the 3rd international workshop on Vehicular ad hoc networks,* Los Angeles, CA, , September 2006.
[24] **C.-T. Li, M.-S. Hwang,** and **Y.-P. Chu**, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications,* vol. 31, pp: 2803-2814, Jan. 2008.
[25] **J. Sun, C. Zhang,** and **Y. Fang**, "An ID-based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks," in *IEEE Military Communications Conference, MILCOM* Orlando, FL, , Oct. 2007, pp: 1-7.
[26] **L. Tim, ller, M. Christian, fer, S. Elmar,** and **K. Frank**, "Improved security in geographic ad hoc routing through autonomous position verification," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks* Los Angeles, CA, USA: ACM, 2006.
[27] **Z. Chenxi, L. Xiaodong, L. Rongxing,** and **H. Pin-Han**, "RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks," in *IEEE International Conference on Communications*, Beijing, May 2008, pp: 1451-1457.
[28] **J. Choi** and **S. Jung**, "A Security Framework with Strong Non-Repudiation and Privacy in VANETs," in *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*, 2009, pp. 1-5.
[29] **Xiong Hu, Qin Zhiguang,** and **L. Fagen**, "Secure Vehicle-to-roadside Communication Protocol Using Certificate-based Cryptosystem," *IETE Technical Review,* vol. 27, pp: 214-219, April 2010.
[30] **G. Yan, S. Olariu,** and **M. C. Weigle**, "Providing VANET security through active position detection," *Computer Communications,* vol. 31, pp: 2883-2897, July 2008.
[31] **M. Eltoweissy, M. H. Heydari, L. Morales,** and **I. H. Sudborough**, "Combinatorial Optimization of Group Key Management," *Journal of Network and Systems Management,* vol. 12, pp: 33-50, 2004.
[32] **M. Moharrum, R. Mukkamala,** and **M. Eltoweissy**, "CKDS: an efficient combinatorial key distribution scheme for wireless ad-hoc networks," in *Performance, Computing, and Communications, 2004 IEEE International Conference on*, 2004, pp: 631-636.
[33] **M. Moharrum, M. Eltoweissy,** and **R. Mukkamala**, "Dynamic combinatorial key management scheme for sensor networks," *Wireless Communications and Mobile Computing,* vol. 6, pp: 1017-1035, 2006.
[34] **H. Arbabi** and **M. C. Weigle**, ""Highway Mobility and Vehicular Ad-Hoc Networks in ns-3," in *Proceedings of the Winter Simulation Conference* Baltimore, MD, 2010.

[35] **A. Wasef, R. Lu, X. Lin,** and **X. Shen**, "Complementing public key infrastructure to secure vehicular ad hoc networks," *Wireless Commun.,* vol. 17, pp: 22-28, 2010.
[36] **M. E. Nowatkowski** and **H. L. Owen**, "Certificate revocation list distribution in VANETs using Most Pieces Broadcast," in *IEEE SoutheastCon 2010 (SoutheastCon), Proceedings of the*, pp: 238-241.
[37] **Roy, B., Barreto, P., Libert, B., McCullagh, N.,** and **Quisquater, J.-J.**, "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps", *Advances in Cryptology - ASIACRYPT 2005,* (Springer Berlin / Heidelberg, 2005), pp: 515-532
[38] **Engoulou, Richard Gilles, Martine Bellaïche, Samuel Pierre,** and **Alejandro Quintero**. "VANET security surveys." *Computer Communications* 44 (2014): 1-13.
[39] **Son, Junggab, Hasoo Eun, Heekuck Oh, Sangjin Kim,** and **Rasheed Hussain**. "Rethinking vehicular communications: merging VANET with cloud computing." *In Proceedings of the 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom),* pp: 606-609. IEEE Computer Society, 2012.
[40] **Alexiou, Nikolaos, Marcello Laganà, Stylianos Gisdakis, Mohammad Khodaei,** and **Panagiotis Papadimitratos**. "VeSPA: vehicular security and privacy-preserving architecture." *In Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy,* pp: 19-24. ACM, 2013.
[41] **Lacroix, Jesse,** and **Khalil El-Khatib**. "Vehicular Ad Hoc Network Security and Privacy: A Second Look." *In VEHICULAR 2014, The Third International Conference on Advances in Vehicular Systems, Technologies and Applications*, pp: 6-15. 2014.
[42] **Daimi, Kevin, Mustafa Saed,** and **Scott Bone.** "A Multi-Level Security Architecture for Vehicular Ad Hoc Network." *In Proceedings of the World Congress on Engineering,* vol. 1. 2014.

جدوى التحقق وتقييم الأداء للقصاء المعتمد على الشبكات المخصصة للمركبات

أحمد الدارايسة، ومحمد محرم*، وأحمد يوسف

قسم نظم المعلومات، جامعة الملك سعود، و عمادة البحث العلمي، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية*

adaraiseh@ksu.edu.sa

المستخلص. إن الشبكات المخصصة للمركبات (فانت، VANETs) هي شبكات لاسلكية تساعد على تحسين الكفاءة والسلامة أثناء القيادة. تقوم هذه الشبكات بتوفير مجموعة واسعة من الخدمات على الطريق مثل الكشف عن الازدحام المروري، وإيجاد طرق بديلة، وتقدير الوقت إلى الوجهة، والتحذير من الاصطدام، وغيرها الكثير. هي واحدة من أكبر التحديات في نشر شبكات الفانت، وكيفية معالجة القضايا الأمنية بنجاح. وترجع هذه القضايا إلى المتطلبات الأمنية المتضاربة مثل الخصوصية وقابلية الكشف. لقد تم اقتراح نظام أمني لهذه الشبكات مبني على الاستبعاد (EBV) كإطار عام لحل بعض القضايا الأمنية للفانت. في هذه الورقة، قمنا بالتحقق من جدوى هذا الإطار وتقييم أدائه من خلال مجموعة من تجارب المحاكاة. لقد قمنا بقياس الوقت اللازم لتسليم الرسائل، وفقدان الحزمة، ومتوسط الإنتاجية. وأظهرت النتائج أن الإطار الجديد منافس قوي للبروتوكولات الأخرى من حيث الكفاءة والتكلفة.

Arabic Section

القسم الإنجليزي

Utilization of the Modern Syllogistic Method in the Exploration of Hidden Aspects in Engineering Ethical Dilemmas

Ali Muhammad Rushdi, Taleb Mansour Alshehri, Mohamed Zarouan, and Muhammad Ali Rushdi*

Department of Electrical and Computer Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah, Kingdom of Saudi Arabia
**Department of Biomedical and Systems Engineering, Faculty of Engineering, Cairo University, Giza, Arab Republic of Egypt*
arushdi@kau.edu.sa

Abstract. Engineering ethical dilemmas emerge as problems that are hard to solve, not due to a deficiency in knowledge of moral rules and principles that are to be referred to, but to other reasons including vagueness, conflict of interest and differences in opinions regarding priorities. This paper proposes utilizing logic deduction in the exploration of hidden aspects in dilemmas, which might lead to their resolution. The paper presents a powerful method for deduction in propositional logic, called the Modern Syllogistic Method. The method ferrets out from a given set of premises all that can be concluded from it in the most compact form. The method casts the set of premises into a single switching function equated to zero and obtains the complete sum of this function as a disjunction of all prime consequents. The complete sum is derived via an efficient method, namely, the improved Blake-Tison algorithm. An incremental version of the MSM augments the original set of premises by new ones, and seeks the updated consequences incrementally, *i.e.*, without having to recalculate the complete sum from scratch. We employ this method in the investigation of different scenarios or premises describing a specific ethical dilemma from a variety of perspectives. Comparison of the consequences of these scenarios helps in deriving acceptable solutions of various dilemmas, including the dilemma of having to pay a bribe to obtain one's own rights, the dilemma of human consumption of genetically-modified foods, and the dilemma of discarding a whole lot of food when only a part of it becomes filthy or unhealthy. The work presented herein is a preliminary step towards implementing a software package that offers assistance in the resolution of ethical dilemmas. The package will use premises that are compatible with the fundamentals and rules of Islamic jurisprudence formulated in deterministic, fuzzy, or intuitionistic fuzzy logic.

[١١٢] **ابن تيمية، أحمد بن عبد الحليم**، *القواعد النورانية الفقهية*، مكتبة السنة المحمدية، القاهرة، مصر، تحقيق **محمد حامد الفقي**، ١٣٧٠هـ/١٩٥١م، الكتاب متاح على الموقع التالي في شبكة الشبكات: http://www.raqamiya.org

[١١٣] **Magrez, P.** and **Philippe, S.**, Fuzzy modus ponens: A new model suitable for applications in knowledge-based systems, *International Journal of Intelligent Systems*, **4** (2): 181-200, (1989).

[١١٤] **Dubois, D.** and **Henri, P.**, Fuzzy logics and the generalized modus ponens revisited, *Cybernetics and Systems*, **15** (3-4): 293-331, (1984).

[١١٥] **Tsukamoto, Y.**, An approach to fuzzy reasoning method, In **Gupta, M. M.** and **Yager, R. R.** (Editors), *Advances in Fuzzy Set Theory and Applications*, North-Holland, Amsterdam, The Netherlands, pp. 137-149, (1979).

[١١٦] **Zadeh, L. A.,** Fuzzy logic, *IEEE Computer*, **21** (4): 83-93, (1988).

[١١٧] **Mizumoto, M.** and **Zimmermann, H.-J.,** Comparison of fuzzy reasoning methods, *Fuzzy Sets and Systems*, **8** (3): 253-283, (1982).

[١١٨] **Hellendoorn, H.**, The generalized modus ponens considered as a fuzzy relation, *Fuzzy Sets and Systems*, **46** (1) 29-48, (1992).

[١١٩] **Gaines, B. R.**, Foundations of fuzzy reasoning, *International Journal of Man-Machine Studies*, **8** (6): 623-668, (1976).

[١٢٠] **Ross, T. J**. *Fuzzy Logic with Engineering Applications*, Wiley, New York, NY,USA, (2009).

[١٢١] **Liu, J., Ruan, D., Xu, Y.** and **Song, Z.**, A resolution-like strategy based on a lattice-valued logic, , *IEEE Transactions on Fuzzy Systems*, **11** (4): 560-567, (2003).

[١٢٢] **Demirli, K.** and **Turksen I. B.,** A review of implications and the generalized modus ponens, *Proceedings of the Third IEEE Conference on Fuzzy Systems* (*IEEE World Congress on Computational Intelligence*), **2**: 1440-1445, (1994).

[١٢٣] **Shen, Zuliang, Liya Ding,** and **Masao Mukaidono.** Fuzzy resolution principle, *Proceedings of the IEEE Eighteenth International Symposium on Multiple-Valued Logic*, pp: 210-215 (1988).

[١٢٤] **Atanassov, K.** and **George, G.,** Elements of intuitionistic fuzzy logic, Part I, *Fuzzy Sets and Systems*, **95** (1): 39-52, (1998).

[١٢٥] **Ciftcibasi, T.** and **Altunay, D.**, Fuzzy propositional logic and two-sided (intuitionistic) fuzzy propositions, *Proceedings of the Fifth IEEE International Conference on Fuzzy Systems,* **1**: 432-438, (1996).

[١٠٠] **Copi, I. M**. and **Cohen, C**., *Introduction to Logic (14th Edition)*, Prentice-Hall, Upper Saddle River, NJ, USA, (2010), 688 p.

[١٠١] **العسقلاني، أحمد بن علي بن حجر**، *فتح الباري شرح صحيح البخاري*، ترقيم: **محمد فؤاد عبدالباقي**، إخراج وتصحيح: **محب الدين الخطيب**، تعليق: **عبدالعزيز بن باز**، دار المعرفة، بيروت، ١٣٧٩هـ، ١٢/٣١٤.

[١٠٢] **الذهبي، عبدالله محمد بن أحمد**، *سير أعلام النبلاء*، تحقيق مجموعة من المحققين بإشراف **شعيب الأرناؤوط**، مؤسسة الرسالة، الطبعة الثانية، ١٤٠٥هـ/ ١٩٨٥م، ٤/٦٠٩.

[١٠٣] **السيوطي، جلال الدين عبدالرحمن بن أبو بكر**، *الأشباه والنظائر في قواعد وفروع فقه الشافعية*، دار الكتب العلمية بيروت – لبنان. الكتاب متاح على الموقع التالي في شبكة الشبكات: http://www.raqamiya.org

[١٠٤] **الزرقا، أحمد محمد**، *شرح القواعد الفقهية*، دار القلم، دمشق، سوريا، ١٤٠٩هـ. الكتاب متاح على الموقع التالي في شبكة الشبكات: http://waqfeya.net/book.php?bid=847

[١٠٥] **ابن رجب الحنبلي، عبدالرحمن بن أحمد**، *القواعد*، الكتاب متاح على الموقع التالي في شبكة الشبكات: http://www.al-islam.com

[١٠٦] **الزحيلي، وهبة**، *الوجيز في أصول الفقه*، دار الفكر، سوريا، ١٩٩٥م.

[١٠٧] **الميداني، عبد الرحمن حبنكة**، *ضوابط المعرفة*، دار القلم، دمشق، سوريا، ١٩٩٣م.

[١٠٨] **الصاعدي، حمد بن حمدي**، *الفرق بين القاعدة الأصولية والفقهية* من خلال التعريف بعلمي أصول الفقه والقواعد الفقهية، *مجلة الجامعة الإسلامية*، العدد ١٣٠، صفحات ٢٩١-٤٢٩ (١٤٢٦هـ).

[١٠٩] **جمعة، عماد علي**، *تشجير روضة الناظر لابن قدامة المقدسي*، دار النفائس للنشر والتوزيع، ٢٠٠٨م.

[١١٠] **آل بورنو، محمد صدقي بن أحمد بن محمد**، الوجيز *في شرح قواعد الفقه* الكلية، مؤسسة الرسالة، بيروت، لبنان، ١٤١٦هـ، الكتاب متاح على الموقع التالي في شبكة الشبكات: http://shamela.ws/index.php/book/8379

[١١١] **جمعة، عماد علي**، *القواعد الفقهية الميسرة*، ٢٠٠٦م، الكتاب متاح على الموقع التالي في شبكة الشبكات: http://ia600507.us.archive.org/2/items/waq110873waq/110873.pdf

[٨٠] **Jackson, P.**, Computing prime implicates incrementally, In *Automated Deduction—CADE-11*, Springer, Berlin-Heidelberg, Germany, pp: 253-267, (1992).

[٨١] **Coudert, O.** and **Madre, J. C.**, Implicit and incremental computation of primes and essential primes of Boolean functions, *Proceedings of the 29th ACM/IEEE Design Automation Conference*, IEEE Computer Society Press, pp: 36-39, (1992).

[٨٢] **Ngair, T.-H.**, A new algorithm for incremental prime implicate generation, *IJCAI*, **1:** 46-51, (1993).

[٨٣] **Dorst**, **K**. and **Royakkers**, **L**., The design analogy: a model for moral problem solving, *Design Studies*, **27:** 633-656, (2006).

[٨٤] **Hatcher, D. L**., Why formal logic is essential for critical thinking, *Informal Logic*, **19** (1): 77-89, (1999).

[٨٥] **Salmon, M.**, *Introduction to Logic and Critical Thinking*, Cengage Learning, Boston, MA,USA, (2012).

[٨٦] **ابن تيمية، أحمد بن عبدالحليم**، *مجموع الفتاوى*، تحقيق: **أنور الباز– عامر الجزار**، دار الوفاء، الطبعة ٣، المجلد ٩، صفحة ٨٢، (١٤٢٦هـ/٢٠٠٥م).

[٨٧] **ابن تيمية، أحمد بن عبدالحليم**، *نقض المنطق*، تحقيق: **محمد بن عبدالرزاق حمزة– سليمان بن عبدالرحمن الصنيع**، صححه: **محمد حامد الفقي**، مطبعة السنة المحمدية، القاهرة، (١٣٧٠هـ/١٩٥١م) (يعرف هذا الكتاب أيضًا باسم "*نقد المنطق*").

[٨٨] **ابن تيمية، أحمد بن عبدالحليم**، *الرد على المنطقيين*، طباعة ونشر: إدارة ترجمان السنة، لاهور، باكستان، (١٣٩٦هـ/١٩٧٦م).

[٨٩] **Heysse, T.**, Why logic doesn‘t matter in the (philosophical) study of argumentation, *Argumentation*, **11** (2): 211-224, (1997).

[٩٠] **Maier, B.** and **W.A. Shibles**, *Medical Language: The Ordinary Language Approach*, Chapter 18 (pp: 427-451) in: *The Philosophy and Practice of Medicine and Bioethics*, Springer Dordrecht Heidelberg, Germany, (2011), 650 p.

[٩١] **Steimann, F**., A case against logic, *Proceedings of the Eighth World Congress on Medical Informatics (MedInfo ´95*), Healthcare Computing & Communications Canada, Inc., Edmonton, Alberta, pp. 989-993, (1995).

[٩٢] **Haack, S**., Dummett's justification of deduction. *Mind*, **91** (362): 216-239, (1982).

[٩٣] **Edmonds, B.,** How formal logic can fail to be useful for modelling or designing MAS, In *Regulated Agent-Based Social Systems*, Springer, Berlin-Heidelberg, pp. 1-15, (2004).

[٩٤] **Sequoiah-Grayson, S.**, The scandal of deduction, *Journal of Philosophical Logic*, **37** (1): 67-94, (2008).

[٩٥] **D'Agostino, M.** and **Floridi, L.**, The enduring scandal of deduction, *Synthese*, **167** (2): 271-315, (2009).

[٩٦] **Copi, I. M.,** *Symbolic Logic* (Fifth edition), Prentice hall, New York, NY, USA, (1979), 411 p.

[٩٧] **Winnie, J. A.,** The completeness of Copi's system of natural deduction, *Notre Dame Journal of Formal Logic*, (**11**): 379-382, (1970).

[٩٨] **Slater, B. H.**, Paraconsistent logics? *Journal of Philosophical logic*, **24** (4): 451-454, (1995).

[٩٩] **Anderson, J. A.,** *Discrete Mathematics with Combinatorics* (Second Edition). Prentice Hall, Upper Saddle River, NJ, USA, (2003), 928 p.

[٦٢] **Hwa, H. R.,** A method for generating prime implicants of a Boolean expression*, IEEE Transactions on Computers,* **C-23** (6): 637-641 (1974).

[٦٣] **Reusch, B.,** Generation of prime implicants from subfunctions and a unifying approach to the covering problem, *IEEE Transaction on Computers*, **C-24** (9): 924-930 (1975).

[٦٤] **Muroga, S.,** *Logic Design and Switching Theory*, Wiley, New York, NY, USA (1979), 618.

[٦٥] **Cutler, R. B.**, **Kinoshita, K.** and **Muroga, S.**, *Exposition of Tison's Method to Derive all Prime Implicants and all Irredundant Disjunctive Forms for a Given Switching Function*, Report No. UIUCDCS-R-79-993, Department of Computer Science, University of Illinois at Urbana-Champaign (UIUC), Urbana, Illinois, IL, USA (1979).

[٦٦] **Loui, M. C, Bilardi, G.,** The Correctness of Tison's Method for Generating Prime Implicants, Report R-952, UILU-ENG 82-2218, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, (UIUC), Urbana, Illinois, IL, USA (1982).

[٦٧] **Coudert, O**., and **Madre, J. C.**, A new method to compute prime and essential prime implicants of Boolean functions, *Advanced Research in VLSI and Parallel Systems, Proceedings of the 1992 Brown/MIT Conference*, **T. Knight** and **J. Savage** (Editors) : 113-128 (1992).

[٦٨] **Rushdi, A. M.** and **Al-Yahya, H. A.,** A Boolean minimization procedure using the variable-entered Karnaugh map and the generalized consensus concept, *International Journal of Electronics,* **87** (7): 769-794*,* (2000).

[٦٩] **Rushdi, A. M.** and **Al-Yahya, H. A.,** Derivation of the complete sum of a switching function with the aid of the variable-entered Karnaugh map, *Journal of King Saud University: Engineering Sciences,***13 (**2): 239-269 (2001).

[٧٠] **Rushdi, A. M.**, Prime-implicant extraction with the aid of the variable-entered Karnaugh map, *Umm Al-Qura University Journal: Science, Medicine and Engineering,* **13** (1): 53-74, (2001).

[٧١] **Rushdi, A. M.** and **Al-Shehri, A. S.,** Selective deduction with the aid of the variable-entered Karnaugh maps, *Journal of King Abdulaziz University: Engineering Sciences,* **15 (** 2): 21-29, (2004).

[٧٢] **Alexe, G.,** **Alexea, S.,** **Crama, Y.,** **Foldes, S.,** **Hammer, P. L.** and **Simeone, B.**, Consensus algorithms for the generation of all maximal bicliques, *Discrete Applied Mathematics*, **145** (1): 11-21 (2004).

[٧٣] **Ślęzak**, **D.,** Association reducts: Boolean representation, in **G. Wang,** ***et al.*** (Editors), *Rough Sets and Knowledge Technology*, RSKT 2006, LNAI 4062, Springer, Berlin-Heidelberg, Germany: 305-312 (2006).

[٧٤] **Pawlak, Z.** and **Skowron, A.**, Rough sets and Boolean reasoning, *Information Sciences*, **177** (1): 41-73 (2007).

[٧٥] **Rushdi, A. M**. and **Albarakati**, **H. M.,** Using variable-entered Karnaugh maps in determining dependent and independent sets of Boolean functions, *Journal of King Abdulaziz University: Computing and Information Technology Sciences,* **1 (**2): 45-67, (2012).

[٧٦] **Rushdi, A. M.** and **Albarakati**, **H. M.,** The inverse problem for Boolean equations, *Journal of Computer Science*, **8** (12): 2098-2105 (2012).

[٧٧] **Rushdi, A. M.**, and **Albarakati**, **H. M.,** Construction of general subsumptive solutions of Boolean equations via complete-sum derivation, *Journal of Mathematics and statistics*, **10** (2): 155-168 (2014).

[٧٨] **Kear, A.** and **Tsiknis**, G., An incremental method for generating prime implicants/ implicates, *Journal of Symbolic Computation*, **9**: 185-206 (1990).

[٧٩] **De Kleer, J.,** An improved incremental algorithm for generating prime implicates, AAAI Press, *of the Tenth National Conference on Artificial Intelligence, Proceedings* (1992).

[٤٥] **Rittel**, **H.** and **M. Webber**, Dilemmas in a general theory of planning, *Policy Sciences*, **4** (2): 155-169, (1973).

[٤٦] **DeGrace**, **P.** and **L. H. Stahl**, *Wicked Problems, Righteous Solutions: A Catalog of Modern Engineering Paradigms*, Prentice-Hall, Upper Saddle River, NJ, USA, (1998).

[٤٧] **رشدي، علي محمد علي**، التفكير الهندسي في استشراف المستقبل، مجلة الملك عبدالعزيز للعلوم الهندسية، ٢٠ (٢)، ١١١-١٤٠ (٢٠٠٩م).

[٤٨] **Blake, A.,** *Canonical Expressions in Boolean Algebra*, Ph. D. Dissertation, Department of Mathematics, University of Chicago (1937), 273 p.

[٤٩] **Brown, F. M.**, *Boolean Reasoning: The Logic of Boolean Equations*, Kluwer Academic Publishers, Boston, MA, USA (1990), 273 p.

[٥٠] **Gregg, J. R.,** *Ones and Zeros*: *Understanding Boolean Algebra, Digital Circuits, and the Logic of Sets*, IEEE PRESS, New York, NY, USA (1998), 296 p.

[٥١] **رشدي، علي محمد علي، والشهري، عبدالرحمن سعيد**، الاستدلال المنطقي ودوره المساند في خدمة الأمن والعدل، *مجلة الدراسات الأمنية*، ١١ (٢٢)، ١١٥-١٥٣ (٢٠٠٢م).

[٥٢] **Rushdi, A. M.** and **Ba-Rukab, O. M.,** Some Engineering Applications of the modern syllogistic method, SEC7 Paper 226, *Proceedings of the 7th Saudi Engineering Conference (SEC7)*, Riyadh, Saudi Arabia, **4**: 389-401 (Also p. 201 in Abstracts Volume) (2007).

[٥٣] **Rushdi, A. M.** and **Ba-Rukab, O. M.,** The modern syllogistic method as a tool for engineering problem solving, *Journal of Qassim University: Engineering and Computer Sciences,* **1** (1): 57-70 (2008).

[٥٤] **Rushdi, A. M.** and **Ba-Rukab, O. M.,** An exposition of the modern syllogistic method of propositional logic, *Umm Al-Qura University Journal: Engineering and Architecture,* **1** (1): 17-49, (2009).

[٥٥] **Rushdi, A. M.,** and **Ba-Rukab, O. M.,** Powerful features of the modern syllogistic method of propositional logic, *Journal of Mathematics and Statistics,* **4** (3): 186-193, (2008).

[٥٦] **Rushdi, A. M.** and **Ba-Rukab, O. M.**, Switching-algebraic analysis of relational databases, *Journal of Mathematics and Statistics*, **10** (2): 231-243, (2014).

[٥٧] **Rushdi, A. M.,** and **Ba-Rukab, O. M.**, Map derivation of the closures for dependency and attribute sets and all candidate keys for a relational database*, Journal of King Abdulaziz University: Engineering Sciences*, **25** (2): 3-33, (2014).

[٥٨] **Rushdi, A. M., Zarouan, M. M.**, **Alshehri, T. M.** and **Rushdi, M. A.** , The Incremental Version of the Modern Syllogistic Method*, Journal of King Abdulaziz University: Engineering Sciences*, accepted for publication.

[٥٩] **Rushdi, A. M., Zarouan M. M.**, **Alshehri, T. M.** and **Rushdi M. A.**, A modern syllogistic method in realistic fuzzy logic*,* submitted for publication.

[٦٠] **Tison, P.,** *Generalization of consensus* theory and application to the minimization of Boolean functions, *IEEE Transactions on Electronic Computers*, **EC-16** (4): 446-456 (1967), with Comments, **Cutler, R. B.** and **Muroga, S.**, *ibid.,* **28** (7) : 542-543 (1979).

[٦١] **Slagle, J. R., Chang, C.-L.** and **Lee, R. C. T.**, A new algorithm for generating prime implicants, *IEEE Transactions on Computers*, **C-19**(4): 304–310 (1970).

[٢٥] **الغزالي، محمد**، *خلق المسلم*، دار الريان للتراث، القاهرة، (١٤٠٨هـ/١٩٨٧م).

[٢٦] **العثيمين، محمد بن صالح**، *مكارم الأخلاق*، مؤسسة الشيخ محمد بن صالح العثيمين الخيرية، الرياض، (١٤٢٨هـ).

[٢٧] **الميداني، عبدالرحمن حبنكة**، *الأخلاق الإسلامية وأسسها*، دار القلم، دمشق، الطبعة الخامسة، (١٤٢٠هـ/١٩٩٩م).

[٢٨] **Von Grunebaum, G. E**., Concept and function of reason in Islamic ethics, *Oriens*, **15**: 1-17 (1962).

[٢٩] **Carney, F. S.**, Some aspects of Islamic ethics, *The Journal of Religion*, **63** (2): 159-174, (1983).

[٣٠] **Kevin Reinhart, A.**, Islamic law as Islamic ethics, *The Journal of Religious Ethics*, **11** (2): 186-203, (1983).

[٣١] **Beekun, R. I.**, *Islamic Business Ethics*, *The International Institute of Islamic Thought*, (1997), 84 p.

[٣٢] **Siddiqui, A.,** Ethics in Islam: Key concepts and contemporary challenges, *Journal of Moral Education*, (1997).

[٣٣] **Sheperd, J. J.,** Islam, in *Encyclopedia of Applied Ethics*, Vol. **2**, San Diego, CA, USA, pp: 733-740, (1998).

[٣٤] **Brown, D**., Islamic ethics in comparative perspective, *The Muslim World*, (1999).

[٣٥] **Ozdemir, I.**, Toward an Understanding of Environmental Ethics from a Qur'anic Perspective, in *Islam and Ecology*: y: *A Bestowed Trust*, **Mathewson, D. F.** and **Bahauddin, A. H**. (Editors), Cambridge: Harvard Divinity School, pp: 3-38, (2003).

[٣٦] **Abdul-Rahman, A. R.,** Ethics in accounting education: Contribution of the Islamic principle of Maslahah, *International Journal of Economics, Management and Accounting*, **11** (1): 1-18, (2003).

[٣٧] **Al-Aqeel, A. I**., Ethical guidelines in genetics and genomics: An Islamic perspective, *Saudi Medical Journal*, **26** (12): 1862-1870, (2005).

[٣٨] **Moad, E. O**., A path to the oasis: Sharī 'ah and reason in Islamic moral epistemology. *International Journal for Philosophy of Religion*, **62** (3): 135-148, (2007).

[٣٩] **Al-A'ali, M.**, Computer ethics for the computer professional from an Islamic point of view, *Journal of Information, Communication and Ethics in Society*, **6** (1): 28-45, (2008).

[٤٠] **Hameed, S. A**., Software engineering ethical principles based on Islamic values. *Journal of Software*, **4** (6): 563-570, (2009).

[٤١] **Abdallah, S.,** Islamic ethics: an exposition for resolving ICT ethical dilemmas, *Journal of Information, Communication and Ethics in Society*, **8** (3): 289-301, (2010).

[٤٢] **Solihu, A. K. H.** and **Ambali, A. R**., Dissolving the engineering moral dilemmas within the Islamic ethico-legal praxes, *Science and Engineering Ethics*, **17** (1): 133-147, (2011).

[٤٣] **Hasan, S.,** Islamic Jurisprudence: Sources and Traditions Creating Diversity in Human Relationships, Chapter 2 in **S. Hasan** (Editor), *The Muslim World in the 21st Century*, Springer Science + Business Media, Heidelberg, Germany, (2012).

[٤٤] **Possumah, B. T., Ismail, A. G**. and **Shahimi, S**., Bringing work back in Islamic ethics. *Journal of business ethics*, **112** (2): 257-270, (2013).

[٦] **Howard, R.**, Fifty-one mini case studies for engineering ethics and professionalism, *Proceedings of the IEEE 26th Annual Conference* on *Frontiers in Education, FIE'96,* **2**: 838-841, (1996).

[٧] **Ertas, A**. and **Jones, J. C.,** Engineering Ethics, Chapter 10 in: *The Engineering Design Process*, Wiley, New York, NY, USA (1993), 525 p.

[٨] **Humphreys, K. K.,** *What Every Engineer Should Know about Ethics* (Vol. **35**), CRC Press, New York, NY, USA, (1999), 264 p.

[٩] **Comstock, G.,** *Vexing Nature?: On the Ethical Case Against Agricultural biotechnology*, Kluwer Academic Publishers, Norwell, MA, USA, (2000), 297p.

[١٠] **Moriarty, G**., Three kinds of ethics for three kinds of engineering. *IEEE Technology and Society Magazine,* **20** (3): 31-38, (2001).

[١١] **Fleddermann, C. B.**, and **Sanadhya, S. K.,** *Engineering Ethics*, Fourth Edition, Pearson Education, Upper Saddle River, MA, USA, (2014), 192 p.

[١٢] **Martin, M. W.,** and **Schinzinger R.**, *Ethics in Engineering*, Fourth Edition, McGraw-Hill, Boston, MA, USA, (2005), 339 p.

[١٣] **Paul**, **R**., and **Elder**, **L**., *The Miniature Guide to Understanding the Foundations of Ethical Reasoning*, Third Edition, Foundation for Critical Thinking, Tomales, CA, USA, 2005.

[١٤] **Atkinson**, **K.** and **Bench-Capon**, **T**., Addressing moral problems through practical reasoning, in **Goble, L**. and **Meyer, J.-J.** (Editors), *Deontic Logic and Artificial Normative Systems*, lecture Notes in Artificial Intelligence (LANI) 3366, pp: 8-23, Springer, Berlin-Heidelberg, Germany, 2006.

[١٥] **رشاد، عصام الدين محمد**، أخلاقيات وآداب العمل في خطط التعليم الهندسي والتقني، سجل البحوث العلمية للمؤتمر الدولي للتعليم الهندسي، ٣٩٢- ٤٠٠ (٢٠٠٦م).

[١٦] **محمد، محمد حسن**، أخلاقيات المهنة: بضاعتنا ردت إلينا، الجامعية: *مجلة جامعة الملك عبدالعزيز*، الصفحتان ٤٠-٤١ (٢٠٠٦م).

[١٧] **Rushdi, A. M.** and **Baz, A. O.,** *Computer assisted resolution of engineering ethical dilemmas*, SEC7 Paper 147, *Proceedings of the Seventh Saudi Engineering Conference (SEC7)*, Riyadh, KSA, pp. 409-418, (2007).

[١٨] **Robbins, R. W.** and **Wallaces, W. A.,** Decision support for ethical problem solving: A multi-agent approach, *Decision Support Systems*, 43: 1571-1587, (2007).

[١٩] **Harris Jr., C., Pritchard, M., Rabins, M. J., James, R.** and **Englehardt, E.,** *Engineering Ethics: Concepts and Cases*, Fifth Edition, Cengage Learning, USA, (2013), 336 pp.

[٢٠] **ابن مسكويه، أبو علي أحمد بن محمد**، *تهذيب الأخلاق*، ت: ٤٢١هـ.

[٢١] **الماوردي، علي بن محمد**، *أدب الدنيا والدين*، ت: ٤٥٠هـ.

[٢٢] **ابن حزم، علي بن أحمد الأندلسي**، *الأخلاق والسير*، ت: ٤٥٦هـ.

[٢٣] **المقدسي، أحمد بن عبد الرحمن بن قدامة**، *مختصر منهاج القاصدين*، مكتبة دار البيان، دمشق، ت: ٦٨٩هـ.

[٢٤] **دراز، محمد عبد الله**، *دستور الأخلاق في القرآن*، مؤسسة الرسالة، الطبعة العاشرة ١٤١٨هـ/ ١٩٩٨م.

وجهات نظرية متباينة. نود في خطوة تالية أن نكرر ذلك مع استخدام مقدمات منضبطة بأصول الفقه الإسلامي وقواعده الفقهية[١٠٣-١١٢] في صور حتمية (Deterministic/crisp) أو في صور يقتضيها المنطق الضبابي (Fuzzy logic)[١١٣- ١٢٣] أو المنطق الضبابي الحدسي (Intuitionistic fuzzy logic)[٥٩، ١٢٤، ١٢٥]. تمهد هذه الدراسات لبناء حزمة برمجية قوية تساعد في حل المعضلات الأخلاقية، ولكن لا تستقل بإجراء الحل بنفسها.

حاولنا خلال عملنا في هذه الورقة دراسة معضلة شائكة التعقيد تتعلق بموضوع قيام موظف يعمل في مؤسسة معينة باللجوء إلى الرأي العام لفضح نوع من الفساد داخل مؤسسته، وهو الأمر الذي اصطلح على تسميته بإطلاق الصَفَّارة أو إطلاق صَفِّارة الانذار (Whistleblowing)[٢]، ومن ثم نسمي هذا الموظف حال إطلاقه الصفارة بالصافر. ولكن اتضح لنا صعوبة المعضلة التي يتناولها هذا المثال مقارنة بالأمثلة الثلاثة التي أوردناها هنا من أمور عدة من بينها الزيادة الواضحة في عدد المتغيرات الإخبارية اللازمة لوصف المسألة، وكذلك كثرة عدد المقدمات المتعين افتراضها، وصعوبة الحصول على نتائج مرضية أيًا كانت مجموعة المقدمات المستخدمة، ولذلك أرجأنا دراسة هذه المسألة إلى عمل مستقبلي مستقل إن شاء الله تعالى.

References

[١] **Rudnicka, E., Besterfield-Sacre, M., Shuman, L.** and **Wolfe, H.**, evaluating the decision making process that individuals and teams of engineering students employ when solving ethical dilemmas, *Proceedings of the IEEE 35th Annual Conference* on *Frontiers in Education, FIE'05,* (Paper T2D-20), (2005).

[٢] **Kumagai, J.**, The whistle-blower's dilemma, *IEEE Spectrum*, **41**(4): 53-55 (2004).

[٣] **Sturges, D. L.**, Overcoming the ethical dilemma: Communication decisions in the ethic ecosystem, *IEEE Transactions on Professional Communication*, **35**(1): 44-50, (1992).

[٤] **Al Ali, B., Mazhar Anwar Ul Haq, M., Al-Rebh, A. A., Al-Qahtani, M.** and **Al-Qurashi, T.,** Decision making in ethical dilemma, *2012 Proceedings of IEEE Technology Management for Emerging Technologies (PICMET'12)*, pp. 589-599, (2012).

[٥] **Unger, S. H.,** Codes of Engineering Ethics, In **Johnson, D. G.** (Editor), *Ethical Issues in Engineering*, Prentice Hall, Englewood Cliffs, NJ, USA, pp: 105-129, (1991).

ثمنه وحده $(\overline{L}_1 = 0)$، أما بقية البراميل التي يُفترض فيها الطهارة فمسكوت عن الطعن في صلاحيتها والمطالبة بسكبها وخسارة ثمنها.

مثال ٣ج:

ندرس هنا الموقف عند بائع من العوام يفتقر إلى العلم الشرعي ولا يعنى بقضايا المفاسد والصحة ونحوها وأكبر همه ومبلغ علمه قد لا يتجاوز أمر الربح والخسارة، ومن ثم فربما لا يعنيه من المقدمات المذكورة في المثال ٣أ غير المقدمتين (3g)، (3h) ونتيجة لحرصه على تفادي الخسارة نضيف المقدمتين:

رقم المقدمة	صياغتها	معناها
(3m)	$\overline{L}_r$	رفض الخسارة الفادحة بفقد ثمن بقية البراميل.
(3n)	$\overline{L}_1$	رفض الخسارة اليسيرة بفقد ثمن البرميل الأول.

هنا تصبح المسألة بسيطة للغاية، وتأخذ الصورة:

$$f_2 \equiv P_1\overline{L}_1 \vee P_r\overline{L}_r \vee L_r \vee L_1 = 0, \qquad (54)$$

والمجموع الكامل لهذه الدالة هو:

$$CS(f_2) \equiv P_1 \vee P_r \vee L_r \vee L_1 = 0. \qquad (55)$$

فهذا البائع الذي كان يخشاه ابن سيرين لن يرضى بخسارة ثمن البرميل الأول $(\overline{L}_1 = 0)$ ولا بخسارة ثمن غيره من البراميل $(L_r = 0)$ ومن ثم فلن يسكب البرميل الأول $(P_1 = 0)$ ولن يسكب غيره من البراميل $(P_r = 0)$. وفي حالة ما ألغينا المقدمة (4n) بافتراض شيء من حسن النية عند البائع فلن نحصل على معلومات عن سكب البرميل الأول، ويصبح هذا الأمر مسكوتا عنه.

٥. خاتمة واستنتاجات

وضحنا في ورقة البحث هذه كيف يمكن توظيف الطريقة الاستدلالية الحديثة لتدارس سيناريوهات مختلفة أو مقدمات مختلفة تصف معضلة أخلاقية معينة من

بأنه مفلس. وخلال سجن ابن سيرين توفي الصحابي الجليل أنس ابن مالك رضي الله عنه خادم النبي صلى الله عليه وسلم، وكان آخر الصحابة موتاً بالبصرة، وأوصى أنس رضي الله عنه أن يغسله ويصلي عليه ابن سيرين، ورضخ والي البصرة آنذاك لهذه الوصية التي تحرمه شخصيا شرفا كان يتمناه (ويستحقه بحكم منصبه) وأخرج ابن سيرين لتلك المهمة بعد استئذان الدائن.

مثال ٣ب:

نعيد حل المسألة السابقة من جهة نظر آخرين لا يرون صحة المقدمتين (3b)، (3i) بل يرون بدلا منها:

رقم المقدمة	صياغتها	معناها
(3k)	$C \rightarrow \overline{(F_1 \longrightarrow F_r)}$	مقتضى عدم زوال اليقين بالشك هو كذب الادعاء بأن نجاسة برميل تقتضي نجاسة بقية البراميل كلها.
(3*l*)	C	اليقين لا يزال بالشك.

تصبح المقدمات في هذه الحالة معطاة بدالة واحدة f_1 مساواة بالصفر هي:

$$f_1 \equiv \overline{F}_1 \vee C(\overline{F}_1 \vee F_r) \vee F_1\overline{N}_1 \vee F_r\overline{N}_r \vee HN_1\overline{P}_1 \vee HN_r\overline{P}_r \vee P_1\overline{L}_1 \vee P_r\overline{L}_r \vee \overline{C} \vee \overline{H} = 0 \quad ,(52)$$

والمجموع الكامل لهذه الدالة هو:

$$CS(f) \equiv \overline{F}_1 \vee F_r \vee \overline{N}_1 \vee \overline{P}_1 \vee N_r\overline{P}_r \vee \overline{L}_1 \vee P_r\overline{L}_r \vee \overline{C} \vee \overline{H} = 0. \qquad (53)$$

وهذه النتيجة تلخص رأي هؤلاء الفقهاء، فهم يتمسكون بأن اليقين لا يزول بالشك $(\overline{C} = 0)$ ويتفقون مع ابن سيرين في ضرورة درء المفسدة المتوقعة $(\overline{H} = 0)$، ومن ثم يعتبرون البرميل الذي وجدت فيه الفأرة نجسا $(\overline{F}_1 = 0)$، ولكن بقية البراميل طاهرة $(F_r = 0)$. ولذلك فالبرميل الأول وحده لا يصلح محتواه للاستهلاك الآدمي $(\overline{N}_1 = 0)$، ومن ثم يسكب وحده $(\overline{P}_1 = 0)$ ويضيع

		البراميل تقتضي سكب محتويات هذه البراميل وعدم إطعامها للناس.
(3g)	$P_1 \longrightarrow L_1$	سكب محتوى البرميل الأول يعني فقدان ثمنه أي خسارة طفيفة.
(3h)	$P_r \longrightarrow L_r$	سكب محتوى بقية البراميل يعني فقدان ثمنه أي خسارة فادحة.
(3i)	D	مطلوب من المرء ترك ما فيه ريبة.
(3j)	H	مطلوب درء مفسدة الإخلال بالصحة العامة.

يمكننا أن نجمع هذه المقدمات في صورة دالة واحدة f نساويها بالصفر على صورة:

$$f = \overline{F}_1 \vee D F_1 \overline{F}_r \vee F_1 \overline{N}_1 \vee F_r \overline{N}_r \vee H N_1 \overline{P}_1 \vee H N_r \overline{P}_r \vee P_1 \overline{L}_1 \vee P_r \overline{L}_r \vee \overline{D} \vee \overline{H} = 0 \quad , \qquad (50)$$

إن المجموع الكامل لهذه الدالة هو:

$$CS(f) \equiv \overline{F}_1 \vee \overline{F}_r \vee \overline{N}_1 \vee \overline{N}_r \vee \overline{P}_1 \vee \overline{P}_r \vee \overline{L}_1 \vee \overline{L}_r \vee \overline{D} \vee \overline{H} = 0 \qquad (51)$$

وهذه النتيجة تلخص موقف ابن سيرين رحمه الله تعالى فهو ترك ما فيه ريبة $(\overline{D} = 0)$ وقد درأ المفسدة المتوقعة $(\overline{H} = 0)$، واعتبر أن النجاسة لا تقتصر على البرميل الأول فحسب $(\overline{F}_1 = 0)$ بل تشمل بقية البراميل أيضا $(\overline{F}_r = 0)$، ومن ثم فعدم الصلاحية للاستهلاك الآدمي لا تتعلق بالبرميل الأول فحسب $(\overline{N}_1 = 0)$ بل تشمل بقية البراميل $(\overline{N}_r = 0)$، ومن ثم فهو لم يكتف بسكب البرميل الأول $(\overline{P}_1 = 0)$ بل سكب بقية البراميل $(\overline{P}_r = 0)$، ومن ثم لم يخسر ثمن البرميل الأول فحسب $(\overline{L}_1 = 0)$ بل خسر ثمن بقية البراميل أيضًا $(\overline{L}_r = 0)$.

لقد ترتب على ورع ابن سيرين إفلاسه، ومن ثم سجنه، ونظر ابن سيرين إلى سجنه كعقوبة طبيعية لذنب كان قد ارتكبه قبل ذلك بأربعين سنة حين عاير رجلا

في الواقع هي حياة أو موت، وأن وجود الفأرة الميتة في الزيت قد يعني تلوثه بجراثيم الطاعون أو غيره من الأمراض الفتاكة.

نصوغ متغيرات المسألة على النحو التالي:

رمز الخبر	معناه
F_1	وجود نجاسة (*Filthiness*) في البرميل الأول (*First*).
F_r	وجود نجاسة في بقية البراميل (*Rest*).
N_1	عدم صلاحية (*Non-edibility*) محتوى البرميل الأول شرعا للاستهلاك الآدمي.
N_r	عدم صلاحية بقية البراميل شرعا للاستهلاك الآدمي.
C	اليقين (*Certainty*) لا يزال بالشك.
D	مطلوب من المرء أن يدع ما يريبه (*Doubt*) إلى ما لا يريبه.
P_1	سكب (*Pouring*) محتوى البرميل الأول.
P_r	سكب محتوى بقية البراميل.
H	درء المفاسد الناجمة عن الإخلال بالصحة (*Health*) العامة.
L_1	الخسارة الطفيفة (*Light loss*) لقيمة الزيت في البرميل الأول.
L_r	الخسارة الفادحة (*Extreme loss*) لقيمة الزيت في بقية البراميل.

يمكننا أن نصف الموضوع من جهة نظر ابن سيرين بالمقدمات التالية:

رقم المقدمة	صياغتها	معناها
(3a)	F_1	توجد نجاسة في البرميل الأول
(3b)	$D \rightarrow (F_1 \longrightarrow F_r)$	مقتضى ترك ما يريب إلى ما لا يريب هو أن نجاسة البرميل الأول تعني نجاسة بقية البراميل.
(3c)	$F_1 \longrightarrow N_1$	نجاسة محتوى البرميل الأول تعني عدم صلاحية هذا المحتوى كطعام للبشر.
(3d)	$F_r \longrightarrow N_r$	نجاسة محتوى سائر البراميل تعني عدم صلاحية هذا المحتوى كطعام للبشر.
(3e)	$HN_1 \longrightarrow P_1$	الحاجة إلى درء المفاسد مع العلم بوجود نجاسة في البرميل الأول تقتضي سكب محتوى البرميل وعدم إطعامه للناس.
(3f)	$HN_r \longrightarrow P_r$	الحاجة لدرء المفاسد مع العلم بمفسدة النجاسة في بقية

وهو ما يعني:

$$\bar{U} = \bar{F} = \bar{H} = \bar{P} = 0. \quad (49)$$

أي أنه في هذه الحالة مع وجود المجاعة، يحدث ضرر حيث يتم انتاج الأطعمة المعدلة الوراثية واستعمالها. وليست هنالك أية معلومات عن المتغير D، أي أننا لا نعرف في هذه الحالة ما إذا كانت تحدث وفيات أو لا.

مثال ٣أ:

نناقش في هذا المثال واقعة تاريخية حدثت للإمام التابعي الجليل محمد بن سيرين رضي الله تعالى عنه نلخصها هنا نقلا عن الإمام الحافظ الذهبي رحمه الله تعالى[١٠٢]. اشترى محمد بن سيرين عددًا من زقاق(١) (براميل) الزيت/ السمن المستخدم كطعام آدمي، وكان الشراء بالأجل أي أنه تسلم السلعة على أن يؤدي ثمنها إلى البائع فيما بعد (عندما ينتهي من بيع السلعة)، وبذا صار الثمن دينًا عليه للبائع. اكتشف محمد بن سيرين فأرة ميتة في أحد البراميل فما كان منه إلا أن سكب البراميل كلها لأنه لم يدر أسقطت الفأرة في هذا البرميل أم أنها سقطت في الصهريج الذي ملئت منه البراميل، وبعبارة أخرى، لم يدر هل النجاسة اقتصرت على برميل واحد أم أنها عمت سائر البراميل. وبرغم أن القاعدة الفقهية تنص على (الأصل بقاء ما كان على ما كان) تفسر هنا باقتصار النجاسة على برميل واحد، إلا أن ورع ابن سيرين منعه من بيع الزيت للناس حتى لا يقع بهم الضرر، كما منعه من رد السلعة للبائع بالعيب الذي فيها حتى لا يبيعها البائع للناس تغريرًا بهم. ويلفت النظر هنا الإيمان المطلق عند ابن سيرين بمقاصد الشريعة الإسلامية وثقته التامة برعايتها لمصالح العباد، فهو لم يكن يعلم من المسألة إلا أنها مسألة نجاسة وطهارة، ولم يكن يعرف ما نعلمه الآن أن المسألة

(١) زقاق: جمع زق، وهو وعاء من جلد أو نحوه يستعمل لحفظ السوائل.

في هذه الحالة، نحصل على المعادلة التالية:

$$f_3 \equiv D \vee \bar{P}\bar{F} \vee U\bar{H} \vee D\bar{H} \vee \bar{P}U \vee \bar{U}F\bar{D} = 0, \qquad (45)$$

هنا يمتص الحد $D\bar{H}$ في الحد D، ويؤدي قانون الانعكاس إلى إحلال الحد $\bar{U}F$ محل الحد $\bar{U}F\bar{D}$، وهذا يولد تراضيًا مع الحد $\bar{P}U$ قيمته $\bar{P}F$ الذي يولد تراضيًا مع الحد $\bar{P}\bar{F}$ قيمته $\bar{P}$، ويقوم هذا الحد الأخير بامتصاص الحدود $\bar{P}F$ و $\bar{P}\bar{F}$ و $\bar{P}U$، وبذلك تنتج النتيجة النهائية:

$$CF(f_3) \equiv D \vee \bar{P} \vee U\bar{H} \vee \bar{U}F = 0. \qquad (46)$$

وهذه النتيجة تتضمن النتائج التالية الجديدة:

$\bar{P} \rightarrow 1$ (يتم إنتاج الأطعمة المعدلة وراثيًا).

$F \rightarrow U$ (وجود مجاعة يقتضي استعمال الأطعمة المعدلة وراثيًا).

مثال ٢هـ:

ماذا يحدث إذا ألغينا المقدمتين الأوليين (2a) و (2b) في المثال (٢أ) واستعملنا مكانهما المقدمتين التاليتين مع الإبقاء على سائر المقدمات:

رقم المقدمة	صياغتها	معناها
(2a")	$D \rightarrow U$	وجود وفيات يقتضي استعمال الأطعمة المعدلة وراثيًا.
(2b")	F	توجد مجاعة.

في هذه الحالة، نحصل على المعادلة التالية:

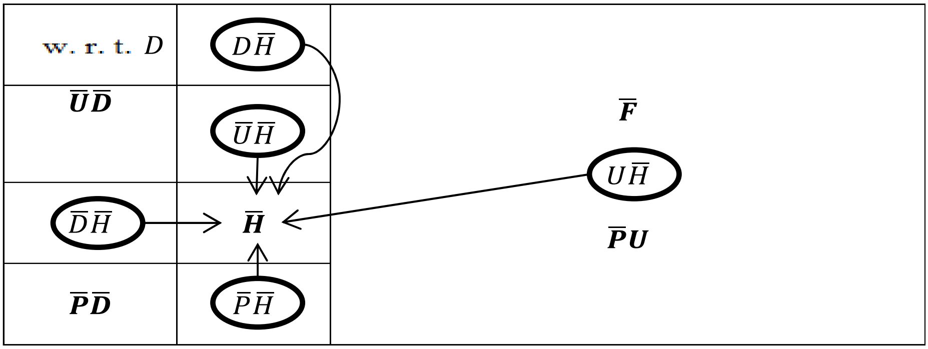
$$f_4 \equiv \bar{U}D \vee \bar{F} \vee U\bar{H} \vee D\bar{H} \vee \bar{P}U \vee \bar{U}F\bar{D} = 0, \qquad (47)$$

هنا يؤدي قانون الانعكاس إلى وضع الحد $\bar{U}D$ محل الحد $\bar{U}F\bar{D}$، وهذا الحد الأخير يندمج مع $\bar{U}D$ ليعطي $\bar{U}$ الذي بفضله يتحول الحدان $U\bar{H}$ و $\bar{P}U$ إلى $\bar{H}$ و $\bar{P}$ وبالتالي يتم امتصاص الحد $D\bar{H}$ لنصل إلى:

$$CF(f_4) \equiv \bar{U} \vee \bar{F} \vee \bar{H} \vee \bar{P} = 0, \qquad (48)$$

w. r. t. U	$U\bar{H}$	$\bar{P}U$	$\bar{F}$ $D\bar{H}$
$\bar{U}F\bar{D}$	$F\bar{D}\bar{H}$	$\bar{P}F\bar{D}$	

w. r. t. F	$\bar{U}F\bar{D}$ ↓	$F\bar{D}\bar{H}$ ↓	$\bar{P}F\bar{D}$ ↓	$U\bar{H}$ $\bar{P}U$ $D\bar{H}$
$\bar{F}$	$\bar{U}\bar{D}$	$\bar{D}\bar{H}$	$\bar{P}\bar{D}$	



شكل (٤). حساب المجموع الكامل للدالة في المثال ٢ج بالنسبة للمتغيرات ثنائية الصيغة U و F و D.

مثال ٢د:

ماذا يحدث إذا ألغينا المقدمتين الأوليين (2a) و (2b) في المثال (٢أ) واستعملنا مكانهما المقدمتين التاليتين مع الإبقاء على سائر المقدمات:

رقم المقدمة	صياغتها	معناها
(2a')	$\bar{D}$	لا توجد وفيات (بدلًا من وجود وفيات).
(2b')	$\bar{P} \rightarrow F$	(عدم انتاج الأطعمة المعدلة وراثيًا يقتضي حدوث مجاعة (بدلًا من الجزم بعدم حدوثها).

مثال ٢د:

ماذا يحدث إذا ألغينا المقدمتين الأوليين (2a) و (2b) في المثال (٢أ) واستعملنا مكانهما المقدمتين التاليتين مع الإبقاء على سائر المقدمات:

رقم المقدمة	صياغتها	معناها
(2a')	$\bar{D}$	لا توجد وفيات (بدلًا من وجود وفيات).
(2b')	$\bar{P} \to F$	(عدم إنتاج الأطعمة المعدلة وراثيًا يقتضي حدوث مجاعة (بدلًا من الجزم بعدم حدوثها).

في هذه الحالة، نحصل على المعادلة التالية:

$$f_3 \equiv D \vee \bar{P}F \vee U\bar{H} \vee D\bar{H} \vee \bar{P}U \vee \bar{U}F\bar{D} = 0, \qquad (45)$$

هنا يمتص الحد $D\bar{H}$ في الحد D، ويؤدي قانون الانعكاس إلى إحلال الحد $\bar{U}F$ محل الحد $\bar{U}F\bar{D}$، وهذا يولد تراضيًا مع الحد $\bar{P}U$ قيمته $\bar{P}F$ الذي يولد تراضيًا مع الحد $\bar{P}F$ قيمته $\bar{P}$، ويقوم هذا الحد الأخير بامتصاص الحدود $\bar{P}F$ و $\bar{P}U$ و، وبذلك تنتج النتيجة النهائية:

$$CF(f_3) \equiv D \vee \bar{P} \vee U\bar{H} \vee \bar{U}F = 0. \qquad (46)$$

وهذه النتيجة تتضمن النتائج التالية الجديدة:

$\bar{P} \to 1$ (يتم إنتاج الأطعمة المعدلة وراثيًا).

$F \to U$ (وجود مجاعة يقتضي استعمال الأطعمة المعدلة وراثيًا).

وهذه نستعمل فيها قانون الانعكاس الذي يضع الحدين U و D محل الحدين $D\bar{H}$ و $U\bar{H}$ ويضع الحد $\bar{U}\bar{D}$ محل الحد $\bar{U}F\bar{D}$، ومن ثم نحصل على القيمة (1) كمجموع للحدود $\bar{U}\bar{D}$ و D و U وبذلك يكون:

$$CS(f_1) \equiv 1 = 0. \qquad (42)$$

أي أن مجموعة المقدمات أصبحت غير متسقة (Inconsistent)، وهو ما يفيد من طرف خفي أنه يتعذر تجنب الضرر مع وجود مجاعة. والواقع أنه لا يمكننا التسليم بوجود هذه المجموعة من المقدمات غير المتسقة وإلا لأمكننا استنباط نتائج متناقضة ولا علاقة لها بالموضوع أصلا.

المثال ٢ ج:

نحاول هنا تعديل المقدمات (2f) –(2a) كما فعلنا في المثال ٢ب بافتراض وجود مجاعة (F) بدلًا من افتراض عدم وجودها، مع التخلي عن فرضية (2a) المتعلقة بانتفاء الضرر. في هذه الحالة نحصل على الشرط:

$$f_2 \equiv F \vee U\bar{H} \vee D\bar{H} \vee \bar{P}U \vee \bar{U}F\bar{D} = 0, \qquad (43)$$

ويوضح الشكل رقم (٤) كيفية حساب المجموع الكامل للدالة f_2 بحساب التراضيات (Consensus terms) بالنسبة للمتغيرات الثلاثة ثنائية الصيغة للحدود U، F، D، حيث نحصل على النتيجة:

$$CS(f_2) \equiv \bar{F} \vee \bar{H} \vee \bar{P}U \vee \bar{U}\bar{D} \vee \bar{P}\bar{D} = 0, \qquad (44)$$

وهذه النتيجة تتضمن بعض النتائج التي تشكل صدى للمقدمات وهي ($\bar{F} = 0$) و ($\bar{P}U = 0$)، كما تتضمن نتائج جديدة هي:

H (يحدث ضرر بسبب نظام التغذية).

$\bar{U} \to D$ (عدم استعمال الأطعمة المعدلة وراثيًا يقتضي حدوث وفيات).

$\bar{P} \to D$ (عدم انتاج الأطعمة المعدلة وراثيًا يقتضي حدوث وفيات).

نفترض صحة المقدمات التالية:

رقم المقدمة	صياغتها	معناها
(2a)	$\bar{H}$	لا يحدث ضرر بسبب نظام التغذية.
(2b)	$\bar{F}$	لا توجد مجاعة بين السكان
(2c)	$U \rightarrow H$	استعمال الأطعمة المعدلة وراثيًا يسبب الضرر.
(2d)	$D \rightarrow H$	حدوث وفيات يعني وقوع ضرر.
(2e)	$\bar{F} \rightarrow \bar{U}$	عدم إنتاج الأطعمة المعدلة وراثيًا يمنع استعمالها.
(2f)	$\bar{U}F \rightarrow D$	عدم استعمال الأطعمة المعدلة وراثيًا في وجود مجاعة يسبب وفيات.

يمكننا أن نجمع هذه المقدمات في صورة دالة واحدة f نساويها بالصفر على صورة:

$$f \equiv H \vee F \vee U\bar{H} \vee D\bar{H} \vee \bar{F}U \vee \bar{U}F\bar{D} = 0, \quad (38)$$

وهذه المعادلة يكفي فيها استعمال قانون الانعكاس (reflection law) لحذف الحرف $\bar{H}$ من الحدين $U\bar{H}$ و $D\bar{H}$، ثم امتصاص الحد $\bar{U}F\bar{D}$ في F وامتصاص الحد $\bar{F}U$ في الحد الجديد U، ومن ثم نحصل على المجموع الكامل:

$$CS(f) \equiv H \vee F \vee U \vee D = 0, \quad (39)$$

وهو ما يعني أن:

$$H = F = U = D = 0. \quad (40)$$

أي أنه يتم تفادي استعمال الأطعمة المعدلة وراثيًا، ولا توجد مجاعة، ولا يحدث ضرر أو وفيات. وهذه الحال مثالية، ولا توجد فيها إشكالات أو معضلات.

المثال ٢ب:

ما الذي يحدث إذا غيرنا الفرضية (2b) التي تقرر عدم وجود مجاعة $(\bar{F})$ إلى الفرضية (F) التي تقرر وجود مجاعة؟ في هذه الحالة نستعمل الدالة f_1 على الصورة:

$$f_1 \equiv H \vee \bar{F} \vee U\bar{H} \vee D\bar{H} \vee \bar{F}U \vee \bar{U}F\bar{D} = 0, \quad (41)$$

ومجموعة النتائج هنا تعني أن دفع الرشوة لتأمين تكليف المهندس بالعمل هو أمر غير أخلاقي، وأن العمل الذي يظفر به المهندس عن طريق الرشوة هو كسب لا يستحقه، بل يسأل عنه في الدارين. ومن المفيد جداً أن نتأمل في الاختلاف بين المثالين (١أ) و(١د) لأنهما وضحا كيف تختلف مذاهب الناس حول نفس القضية بسبب اختلاف تصوراتهم الأصلية عن المسألة نفسها، حيث يتمثل هذا الاختلاف في فروق قد تكون طفيفة في بعض المقدمات التي تصف المسألة.

نلاحظ أن نتائج هذا المثال تنطبق على قضية أكثر أهمية من قضية الارتشاء، ألا وهي قضية *التقية* (religious dissimulation)، وهي رخصة تسمح للمرء باتقاء الضرر وذلك بالحذر من إظهار ما في النفس من معتقد وغيره للغير[١٠١]، إذ يرخص للمسلم أن يستخدم التقية دون توسع فيها وفقط عند الضرورة المؤكدة وبضوابط معينة. وعدم الأخذ بهذه الرخصة أفضل لأصحاب العزيمة بل هي واجب لا محيص عنه للأئمة المقتدى بهم. ومشهور موقف الإمام الفاضل أحمد بن محمد بن حنبل رضي الله عنه يوم المحنة حيث رفض أن يترخص رأفة بنفسه حتى لا يتسبب في إضلال جمهور الناس من العوام.

مثال ٢أ:

يتعلق هذا المثال بالأطعمة المعدَّلة وراثيًا (genetically-modified foods)، حيث توجد معضلة أنَّ هذه الأطعمة تسبب أضرارًا للبشر، وفي نفس الوقت، قد لا يتسنى الاستغناء عنها لتفادي المجاعات. نفترض أن لدينا المتغيرات الإخبارية التالية:

رمز الخبر	معناه
P	إنتاج (*Production*) الأطعمة المعدلة وراثيًا.
U	الاستعمال (*Usage*) البشري للأطعمة المعدَّلة وراثيًا.
F	وجود نقص فادح في الموارد الغذائية يسبب المجاعة (*Famine*).
D	حدوث وفيات (*Deaths*) بين السكان راجعة إلى نظام التغذية.
H	وقوع ضرر (*Harm*) بين السكان راجع إلى نظام التغذية.

وهذه النتيجة الأخيرة تعني أن مجموعة المقدمات أصبحت غير متسقة (Inconsistent) وهو أمر لا يمكن قبوله، لأن مجموعة المقدمات غير المتسقة يمكن استخدامها لإثبات أية نتيجة تخطر على البال حتى وإن كانت لا صلة لها بالمقدمات مثل "الأرض تدور حول الشمس"، وكذلك لإثبات النتيجة المضادة مثل " الأرض لا تدور حول الشمس". إن نتيجة هذا المثال توضح لماذا تمثل المشكلة التي نحن بصددها معضلة أخلاقية (Ethical dilemma)، حيث لا يتسنى لنا أن نضع ما نشاء من مقدمات، لأن فساد المسؤول لا يسمح للمهندس أن يجمع بين مطلب الحصول على حقه في العمل ومطلب الالتزام الأخلاقي بعدم دفع الرشوة.

مثال ١د:

إن النتيجة التي وصلنا إليها في المثال ١أ مسببة لنوع من الإحباط وليس من الميسور التسليم بها، فإنه إن جاز لعوام الناس الترخص في دفع الرشوة عند الضرورة القهرية لاستخلاص حقوقهم، إلا أن ذلك الترخص لا يستساغ أو لا يقبل من أصحاب العزيمة أو علو الهمة أو شدة الورع مثل الأئمة المقتدى بهم، ولذلك أضفنا المقدمة التالية إلى المقدمات التسع في المثال ١أ:

رقم المقدمة	صياغتها	معناها
(1m)	$B \to \bar{E}$	دفع الرشوة غير مقبول أخلاقيًا.

وبرغم أن هذه المقدمة قريبة الشبه من المقدمة (1/) في المثال ١ج، إلا أنها تختلف عنها في أنها لا تؤدي إلى عدم اتساق مجموعة المقدمات الكلية، إذ إنها تسفر عن المعادلة التالية لمجموعة المقدمات الكلية الجديدة:

$$f_3 = f \vee BE = 0, \quad (37a)$$
$$f_3 = CS(f) \vee BE = 0, \quad (37b)$$
$$f_3 = H \vee \bar{W} \vee \bar{B} \vee D\bar{E} \vee \bar{D}E \vee BE = 0, \quad (37c)$$
$$CS(f_3) = H \vee \bar{W} \vee \bar{B} \vee E \vee D = 0. \quad (37d)$$

Consensi/W	$\bar{H}W\bar{B}$	$WD\bar{E}$	$W\bar{D}E$	$D\bar{B}W$	$\boldsymbol{H}$
$\boldsymbol{\bar{W}}$	$\boldsymbol{\bar{H}\bar{B}}$	$\boldsymbol{D\bar{E}}$	$\boldsymbol{\bar{D}E}$	$\boldsymbol{D\bar{B}}$	

Consensi/ D	$\boldsymbol{D\bar{E}}$	$\boldsymbol{D\bar{B}}$	$\boldsymbol{H}$ $\boldsymbol{\bar{W}}$ $\boldsymbol{\bar{H}\bar{B}}$
$\boldsymbol{\bar{D}E}$	---	$\boldsymbol{\bar{B}E}$	

Consensi/ H	$\boldsymbol{H}$	$\boldsymbol{D\bar{E}}$ $\boldsymbol{\bar{D}E}$ $\boldsymbol{\bar{W}}$ $D\bar{B}$ $\bar{B}E$
$\bar{H}\bar{B}$	$\boldsymbol{\bar{B}}$	

Consensi/ E	$\boldsymbol{D\bar{E}}$	$\boldsymbol{\bar{B}}$ $\boldsymbol{\bar{W}}$ $\boldsymbol{H}$
$\boldsymbol{D\bar{E}}$	---	

شكل (٣). حساب المجموع الكامل للدالة $\boldsymbol{f}$ المعطاة في المعادلة (25) في المثال ١أ بالنسبة للمتغيرات ثنائية لصيغة $\boldsymbol{W}$ و $\boldsymbol{D}$ و $\boldsymbol{H}$ و $\boldsymbol{E}$.

$$f_1 = CS(f) \vee \bar{W}DH \vee \bar{W}\bar{D}\bar{H} = 0, \quad (32)$$

$$f_1 = H \vee \bar{W} \vee \bar{B} \vee D\bar{E} \vee \bar{D}E \vee \bar{W}DH \vee \bar{W}\bar{D}\bar{H} = 0, \quad (33)$$

ونلاحظ أن الحد $\bar{W}DH$ يحتوي الحد $\bar{W}$ حرفيًا ومن ثمَّ يمتص به، كما أن الحد $\bar{W}\bar{D}\bar{H}$ أيضًا يحتوي الحد $\bar{W}$ حرفيًا وبالتالي يمتص فيه، ولذلك ينشأ أن:

$$CS(f_1) = CS(f), \quad (34)$$

وهو ما يعني أن نواتج المسألة تبقى على حالها ولا تتغير بإضافة المقدمتين (1j) و(1k). إن هاتين المقدمتين متضمنتان (بصورة قد تكون خفية بعض الشيء) في مجموعة المقدمات الأصلية، ولكن هذا التضمن لم يصبح جليًا إلا من خلال صياغة المعادلات (31) – (34).

مثال ١ج:

مرة أخرى، تمَّ اقتراح مقدمة جديدة تضاف إلى المقدمات التسع (1a) – (1i) في المثال ١أ. هذه المقدمة هي:

رقم المقدمة	صياغتها	معناها
$(1l)$	$\bar{B}$	لا يدفع المهندس الرشوة.

هذه المقدمة تأخذ الصورة الصفرية:

$$\bar{B} = 0, \quad (35)$$

وبها تصبح المعادلة المعبرة عن المقدمات الكلية هي:

$$f_2 = f \vee B = 0, \quad (36a)$$

$$f_2 = CS(f) \vee B = 0, \quad (36b)$$

$$f_2 = H \vee \bar{W} \vee \bar{B} \vee D\bar{E} \vee \bar{D}E \vee B = 0, \quad (36c)$$

$$CS(f_2) = 1 = 0. \quad (36d)$$

تتضمن المعادلة (28) صدى لبعض المقدمات حيث تفيد أن المسؤول ليس أميناً، وأنه يمنح العمل للمهندس، كما تتضمن معلومات كانت مخفية في المقدمات، وهي أن المهندس يدفع رشوة للمسؤول، وأن المسلك الأخلاقي للمهندس يتوقف على مدى استحقاقه للعمل، فإن كان مستحقًا للعمل كان مسلكه أخلاقيًا، وإن كان غير مستحق كان مسلكه غير أخلاقي. وهذه النتيجة الأخيرة تتفق مع الرأي الراجح في الفقه الإسلامي الذي يرى أن الضرورات تبيح المحظورات، ولذلك يرخص للإنسان في دفع الرشوة (رغم كونها محرمة في الأصل) إذا لم يجد سبيلاً لاستخلاص حقه بدونها. وبطبيعة الحال، فإن مسألة الترخيص في الرشوة قد لا تكون مقبولة نظاميًا أو قانونيًا في بلدان كثيرة.

مثال ١ب:

في المسألة السابقة قد يقال إن مجموعة المقدمات غير كافية لوصف المسألة، وإن هنالك مقدمتين إضافيتين يتعين إلحاقهما بمجموعة المقدمات الأصلية وهما:

رقم المقدمة	صياغتها	معناها
(1j)	$\overline{W} D \rightarrow \overline{H}$	عدم تكليف المهندس بالعمل رغم كونه مستحقًا له يعني عدم أمانة المسؤول.
(1k)	$\overline{W}\,\overline{D} \rightarrow H$	عدم تكليف المهندس بالعمل عند عدم استحقاقه له يعني أمانة المسؤول.

يمكن ترجمة هاتين المقدمتين إلى معادلتين صفريتين على الصورة:

$$\overline{W} D H = 0, \quad (29)$$

$$\overline{W}\,\overline{D}\,\overline{H} = 0, \quad (30)$$

ومن ثمَّ تؤول المعادلة المعبرة عن المقدمات الكلية إلى:

$$f_1 = f \vee \overline{W} D H \vee \overline{W}\,\overline{D}\,\overline{H} = 0, \quad (31)$$

وهذه يمكن أن تكتب على الصورة:

أية أهمية للمقدمة الخامسة (1e) المشروطة بعدم حصوله على العمل، أو للمقدمة التاسعة (1i) التي تحدد شرطاً للحصول على العمل، كما أن هذا الحصول يعدل المقدمة الرابعة (1d) لتجعل انعدام الأمانة يقتضي الرشوة أو جحود العمل أو يقتضيهما كليهما:

رقم المقدمة	صياغتها	معناها
(1d')	$\bar{H} \to (B \vee \bar{W})$	انعدام الأمانة يقتضي الرشوة أو جحود العمل أو يقتضيهما كليهما.

وبمعنى آخر فإن الحد $\bar{W}$ يمتص كلاً من الحدود $\bar{W}E$ ، $B\bar{W}$، $\bar{H}\bar{W}B$.

وبذلك تتحول المعادلة (25) إلى:

$$ABC(f) = H \vee \bar{W} \vee \bar{H}W\bar{B} \vee WD\bar{E} \vee W\bar{D}E \vee D\bar{B}W = 0. \quad (26)$$

يوضح الشكل رقم (٣) حساب المجموع الكامل لهذه الدالة باستخدام طريقة بليك– تايسون المحسنة (Improved Blake-Tison Method)[٥٨، ٦٩] بالنسبة لكل متغير من المتغيرات الأربعة ثنائية الصيغة (biform) وهي المتغيرات W و D و H و E التي يظهر كل منها في الصيغة الموجبة أو المثبتة (Un-complemented) وأيضًا في الصيغة السالبة أو المنفية (complemented).

ينتج من الشكل رقم (٣) أن:

$$ABC(f) = H \vee \bar{W} \vee \bar{B} \vee D\bar{E} \vee \bar{D}E = 0, \quad (27)$$

ومنها ينتج أن:

$$H = 0,\ W = B = 1, D \equiv E\,, \quad (28)$$

يمكن أن نصف الموقف المذكور بالمقدمات التالية:

رقم المقدمة	صياغتها	معناها
(1a)	$\bar{H}$	المسؤول ليس أمينًا.
(1b)	W	يُوكل المسؤول العمل للمهندس.
(1c)	$H \rightarrow (W \equiv D)$	الأمانة تقتضي إعطاء العمل للمهندس إذا وفقط إذا كان مستحقًا له.
(1d)	$\bar{H} \rightarrow (W \equiv B)$	انعدام الأمانة يقتضي إعطاء العمل للمهندس إذا وفقط إذا دفع الرشوة.
(1e)	$\bar{W} \rightarrow E$	إذا لم يحصل المهندس على العمل فلا مطعن ولا مؤاخذة ولا اتهام له أخلاقيا.
(1f)	$WD \rightarrow E$	إذا حصل المهندس على العمل وكان مستحقاً له فإنه لم يخل بمتطلبات السلوك الأخلاقي.
(1g)	$W\bar{D} \rightarrow \bar{E}$	إذا حصل المهندس على العمل دون أن يكون مستحقاً له، كان مسلكه غير أخلاقي
(1h)	$D\bar{B} \rightarrow \bar{W}$	إذا استحق المهندس العمل ولم يدفع الرشوة، فإن العمل لا يُوكل له.
(1i)	$B \rightarrow W$	دفع الرشوة يؤمن حصول المهندس على العمل.

يمكننا أن نجمع هذه المقدمات في صورة دالة واحدة f نساويها بالصفر على صورة:

$$f = H \vee \bar{W} \vee H(W\bar{D} \vee \bar{W}D) \vee \bar{H}(W\bar{B} \vee \bar{W}B) \vee \bar{W}\bar{E} \vee WD\bar{E} \vee W\bar{D}E \vee D\bar{B}W \vee B\bar{W} = 0 \quad (25)$$

نلاحظ أن المقدمة الثالثة عن مقتضيات الأمانة (1c) لا طائل منها طالما أن المسؤول ليس أمينًا، ولذا فإن الحد المعبر عنها في المعادلة (25) سيمتص في الحد H. بالمثل، فإن حصول المهندس على العمل (المقدمة الثانية (1b)) يلغي

نظير خاطئ شهير على الصورة:

$$\{\overline{A} \rightarrow \overline{B}, A\} \rightarrow \{B\}, \qquad \text{(WRONG)} \qquad (22)$$

وما هذا إلا مغالطة منطقية تسمى مغالطة المعكوس (Inverse fallacy)[٩٩] أو مغالطة إنكار المقدمة (Fallacy of denying the antecedent)[١٠٠]. مرة أخرى تسعفنا ط د ح في إبطال هذه المغالطة سريعا لأنها تصوغ مقدمتيها على الشكل:

$$f = \overline{A}B \vee \overline{A} = 0, \qquad (23)$$

ومن ثم تتوصل إلى:

$$CS(f) - \overline{A} - 0, \qquad (24)$$

وبذا يتضح أن المقدمتين لا تدعمان غير النتيجة $\{A\}$ التي لا تتضمن النتيجة المزعومة $\{B\}$.

٤. أمثلة لتدارس المعضلات الأخلاقية بالطريقة الاستدلالية الحديثة

مثال ١أ:

يحاول مهندس استشاري الحصول على عمل من إحدى الجهات الحكومية، إلا أن المسؤول المختص يرفض أن يوكل إليه العمل ما لم يدفع إليه رشوة معينة، فهل من المقبول أخلاقياً أن يدفع المهندس الرشوة حتى يحصل على العمل؟ نقوم بتعريف الأخبار (Propositions) التالية:

رمز الخبر	معناه
W	يُوكل المسؤول العمل (*Work*) إلى المهندس.
D	المهندس مستحق (*Deserving*) أن يُوكل إليه العمل.
H	المسؤول أمين (*Honest*).
E	سلوك المهندس أخلاقي (*Ethical*).
B	يدفع المهندس الرشوة (*Bribe*) إلى المسؤول.

توليدها صادقة أصلا و(ب) كون قواعد الاستدلال المستخدمة في توليدها سليمة. شاع استخدام قواعد استدلال مزعومة غير سليمة من الناحية الرياضية برغم أنها قد تشبه نوعًا ما قواعد الاستدلال السليمة، ومن ثم فقد تنطلي على غير المتخصصين، وتعرف هذه القواعد الكاذبة بالمغالطات المنطقية (Logical fallacies).

أشهر قواعد الاستدلال هي طريقة الوضع (Modus Ponens)

$$\{A \to B, A\} \to \{B\}, \qquad (17)$$

لها نظير خاطئ شهير على الصورة

$$\{A \to B, B\} \to \{A\}, \quad \text{(WRONG)} \qquad (18)$$

وهذا النظير هو مغالطة منطقية تسمى مغالطة العكس (Converse fallacy)[٩٩] كما تسمى مغالطة إثبات النتيجة (Fallacy of affirming the consequent)[١٠٠]. إن ط د ح سريعة في دحض وإبطال هذه المغالطة لأنها تصوغ مقدمتيها في صورة المعادلة:

$$f = A\overline{B} \vee \overline{B} = 0, \qquad (19)$$

ومن ثم نتوصل إلى:

$$CS(f) = \overline{B} = 0, \qquad (20)$$

وبالتالي يتضح أن المقدمتين لا تدعمان سوى النتيجة $\{B\}$، وأما النتيجة المزعومة $\{A\}$ فلا يتسنى إثبات صحتها من $\{B\}$. وبالمثل نلاحظ أن لطريقة الرفع (Modus Tollens):

$$\{A \to B, \overline{B}\} \to \{\overline{A}\}, \qquad (21)$$

تجربة شهيرة قبيل مطلع القرن العشرين الميلادي) لا زالت تعيش في أذهان الكثير من إعلامينا، حين يبعثون إلينا بكلامهم عبر ما يسمونه "الأثير".

إن مناقشتنا السابقة توضح كيف تعالج ط د ح بعض غرائب وأعاجيب المنطق الاستنباطي التي يترصدها خصومه، فإنها تحصن مستخدميها من الوقوع في فخ استخدام مقدمات غير متسقة لاستنباط نتيجة مرغوب فيها، وكيف تعزز قدرتهم على كشف مخادعة الآخرين لهم باستنباط ما يريدون من مقدمات غير متسقة. إن فعالية الطريقة في الحالتين هي إظهار ما يكون مخفيًا من عدم الاتساق من خلال إثبات أن $\{CS(f) = 1\}$. وفي هذه الحالة يتعين على المستخدم أن يمتنع تماما عن أن يستنبط شيئا من مجموعة المقدمات المعطاة. ويحسن به أن يراجع المقدمات ويغير بعضها للحصول على مجموعة متسقة. ثمة مجال علمي واسع يجري فيه معالجة المجموعة غير المتسقة وجعلها شبه متسقة (Para-consistent) ومحاولة الانتفاع بها على حالها. وهذا المجال (الذي يخرج عن نطاق المنطق الإخباري وطرائقه ومنها طريقة ط د ح) يعرف باسم "المناطق شبه المتسقة (Para-consistent logics)"[٩٨]. ويبدو لنا أن الأقدمين اعتبروا كلمة "المنطق" (logic) ملازمة للإفراد ولا جمع لها، ولكن في التوجه الحديث لم يعد المنطق كينونة واحدة بل تعددت المناطق (Logics)، وقد استخدمنا هنا الجمع القياسي لوزن مفعِل على مفاعل. ولا ضير أن تكون "مناطق" جمعًا لكل من "منطق" و"منطقة" فذلك على غرار كون "مواقع" جمعًا لكل من "موقع" و"موقعة".

٣-٣ إبطال المغالطات المنطقية

تاريخيًا، لم يستعمل المنطق لعمل الاستنباطات السليمة فحسب بل استعمل أيضًا لترويج الأباطيل في صورة مستنبطات تبدو كما لو كانت صحيحة. لا يمكن أن تكون النتائج المستنبطة صادقة إلا في حال (أ) كون المقدمات المستخدمة في

وهو شرط جلي التناقض. نلاحظ أن المقدمات غير المتسقة (مهما كانت درجة خفاء عدم اتساقها) تنتهي مع ط د ح إلى الشرط (16) الذي يعني بوضوح أن مجموعة المقدمات ذاتية التناقض (Self-contradicting)، وأن خبر العطف بين أخبارها متيقن الكذب بحيث يستحيل أن نعين قيما محددة للمتغيرات المعنية تجعل جميع المقدمات صادقة في آن واحد. ومن غرائب المنطق الاستنباطي أن عدم اتساق مجموعة المقدمات يكافئ صدق جميع النتائج أيا كانت {وهذا ما تدل عليه ط د ح لأن أي مضروب يحتوي حرفيا (Subsumes) المضروب 1}. إن استخدام مجموعة مقدمات غير متسقة من أشهر الوسائل للخداع باسم المنطق، حيث يمكن استخدام مثل هذه المجموعة (مع تحبيذ أن يكون عدم اتساقها خفيا) لإثبات أية نتيجة يراد إثباتها، حتى لو كانت لا علاقة لها البتة (Totally irrelevant) بموضوع المقدمات. وأعجب من ذلك أن مجموعة المقدمات غير المتسقة يكمن أن تستخدم لإثبات أي خبر ونقيضه في آن واحد. ويمكن للقارئ الرجوع إلى بحث عن ط د ح كأداة لحل المشاكل الهندسية[٥٣]، حيث يتحدث المثال ٣ عن مفاوضات تجري بين مهندس وإدارة شركته حول مكافأة نهاية الخدمة المستحقة له، وتأخذ المفاوضات طريقا مسدودا حين تفرض الإدارة مجموعة كبيرة من المقدمات غير المتسقة التي يخفى عدم اتساقها، ثم تستنبط منها ما يحلو لها من نتائج، ويوضح المثال كيف يمكن أن يستعمل المهندس ط د ح لكشف التناقض ودفع الظلم الذي يستهدفه. يقدم رشدي وباركب[٥٥] مثالين آخرين على استعمال ط د ح في كشف زيف بعض الافتراضات العلمية التي كانت سائدة في القرن التاسع عشر الميلادي، ومنها فرضية وجود مادة الفلوجيستون (Phlogiston) لتفسير ظاهرة الاحتراق وفرضية وجود مادة الإثير (Ether) لتفسير امتداد الموجات الكهربائية المغناطسية في الفراغ. والطريف أن فرضية وجود الأثير (التي حطمتها

$$CS(f) = A\overline{B} \vee C\overline{D} \vee \overline{A}\,\overline{C} \vee \overline{B}\,\overline{C} \vee \overline{A}\,\overline{D} \vee \overline{B}\,\overline{D} = 0 \quad , \qquad (14)$$

وبذلك فإن الطريقة الاستدلالية الحديثة تقول إن نتائج المعضلة البناءة تشمل فضلا عن نتيجتها النهائية جميع مقدماتها (وهذا معلوم بالضرورة عندما تكون المقدمات من الضامنات الأولية) بالإضافة إلى نتيجتين وسطيتين هما $(B \vee C)$ و$(A \vee D)$. إن ما يسمى بالنتيجة النهائية للقاعدة هو أقوى النتائج الممكنة أي هو آخر النتائج ظهورًا خلال عملية الاستنباط، ومن ثم فهو لا ينبني على المقدمات مباشرة وإنما يتطلب صحة النتائج الوسيطة أيضًا.

٢-٣ القدرة على كشف عدم الاتساق

تتمتع الطريقة الاستدلالية الحديثة بمقدرة ذاتية على الكشف عن وجود عدم اتساق أو تناقض في مجموعة معطاة من المقدمات، وفي التصريح بالتداعيات الناشئة عن عدم الاتساق هذا.

نلاحظ أنه إذا كانت مجموعة المقدمات غير متسقة، فإن نتيجة العطف (Conjunction) بين أخبارها تعطي الخبر متيقن الكذب (False) أي القيمة المنطقية 0. وهذا يعني أن الدالة f محل الدراسة تكون لها القيمة المنطقية 1، غير أن ذلك لا يتضح عادة من التعبير الرياضي المتوفر لهذه الدالة. إن الطريقة الاستدلالية الحديثة تقوم في إجرائها الاعتيادي بحساب صيغة المجموع الكامل للدالة $CS(f)$، ومن ثم تحول أية تعبير رياضي معطى للدالة f (ذات القيمة 1 الخفية) إلى القيمة 1 صراحة، أي أنها تصل إلى النتيجة:

$$CS(f) = 1, \qquad (15)$$

وإذا دمجنا هذه النتيجة مع المعادلة (10)، نحصل على الشرط:

$$1 = 0, \qquad (16)$$

من المقدمات، أو بعبارة أدق أنها تسمح بإنشاء برهان صوري لصحة أية قضية صحيحة. قبل عقود من الزمان، كان المفهوم أن نظامًا كاملًا للاستنباط الطبيعي (Natural deduction) يمكن أن يتشكل من عشر من قواعد الإحلال مضافا إليها بعض قواعد الاستدلال[٩٦، ٩٧]. يمكننا أن نبرهن على كمال الطريقة الاستدلالية الحديثة من كونها تستخدم ضمنًا جميع قواعد الإحلال فضلاً عن أنها تبرهن على صدق جميع قواعد الاستدلال[٥٥]. والمتأمل في البرهان الخاص بقاعدة الوضع (Modus Ponens)[٥٥] (وبعض قواعد الاستدلال الأخرى) يجد أن فكرة توليد التراضيات (Consensus generation) الجوهرية في الطريقة الاستدلالية الحديثة كامنة في هذه القواعد.

ثمة ملحوظة مهمة، وهو أن بعض قواعد الاستدلال الشهيرة لها نتائج متعددة لا تقتصر على النتيجة الوحيدة التي تنسب لها. وعلى سبيل المثال فإن القاعدة المعروفة باسم "المعضلة البناءة" (Constructive dilemma) لها المقدمات $(A \to B)$ و $(C \to D)$ و $(A \vee C)$ ينسب لها نتيجة واحدة هي $(B \vee D)$، ولكن ط دح تضع المقدمات في صورة المعادلات الصفرية:

$$A\overline{B} = 0, \tag{12a}$$

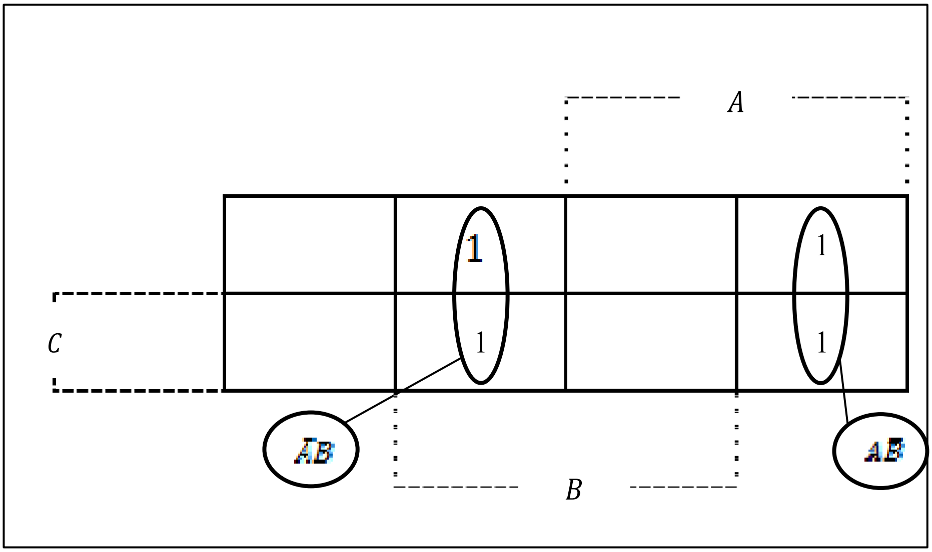
$$C\overline{D} = 0, \tag{12b}$$

$$\overline{A}\,\overline{C} = 0, \tag{12c}$$

ومن ثم تجمعها في معادلة صفرية واحدة.

$$f = A\overline{B} \vee C\overline{D} \vee \overline{A}\,\overline{C} = 0, \tag{13}$$

ثم نشتق المجموع الكامل للدالة f السابقة على الصورة



(ج) المضروبان $A\bar{B}$ و$\bar{A}B$ بينهما أكثر من تضارب (تضاربان اثنان في هذه الحالة)، وتمثلهما حلقتان غير متداخلتان متباعدتان (لا حدود مشتركة بينهما)، ومن ثم يقال إن تراضيهما هو الصفر أو إنه لا تراضي بينهما.

شكل (٢). توضيح تصويري لحقيقة أن مضروبين يولدان تراضيًا إذا وفقط إذا كان بينهما تعارض واحد.

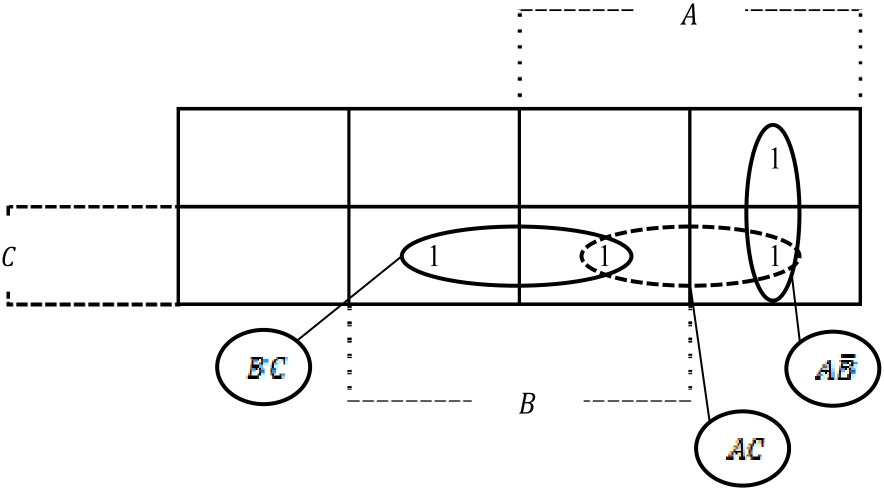
٣. خصائص الطريقة الاستدلالية الحديثة (ط د ح)

فيما يلي نسرد بعض الخصائص المهمة للطريقة الاستدلالية الحديثة في المنطق الإخباري:

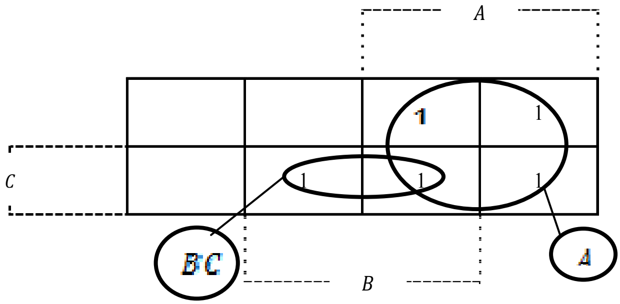
٣-١ طريقة كاملة (Complete)

إن الطريقة الاستدلالية الحديثة هي طريقة كاملة للاستنباط المنطقي بمعنى أنها كافية (Sufficient) بذاتها لاستنباط كل ما يمكن استنباطه من أية مجموعة

غير مكتملة بحيث لا تكفي لإثبات النتيجة المقترحة. وكل ما يمكن قوله في هذه الحالة هو أن مجموعة المقدمات المعطاة لا تؤيد أو لا تدعم النتيجة المقترحة.



(أ) المضروبان $A\bar{B}$ وBC لهما تضارب واحد، وتمثلهما حلقتان غير متداخلتين متشاركتان في حدودهما عند الحد الفاصل بين B و$\bar{B}$، ومن ثم فيمكن أن نضيف إلى اتحادهما التراضي AC.



(ب) المضروبان A وBC لا تضارب بينهما وتمثلهما حلقتان متداخلتان، ومن ثم يقال إن تراضيهما هو الصفر أو إنه لا تراضي بينهما.

احتواءه على ضامنات غير أولية، أما عملية توليد وإضافة التراضي فتؤدي على النقيض من ذلك إلى تكبير حجم مجموع المضروبات المعبر عن f، وهي ضرورية لمنع خلوه من بعض الضامنات الأولية.

٤- بعد الحصول على الدالة في صورة المجموع الكامل أي مجموع جميع ضامناتها الأولية، نساوي كل حد في هذا المجموع (أي كل ضامن أولي) بالصفر المنطقي فنحصل على جميع النتائج التي يمكن استنباطها من المعطيات وفي أبسط صورة ممكنة، أي نحصل على:

$$CS(f) = \bigvee_{i=1}^{\ell} P_i = 0, \tag{10}$$

ومن ثم يكون

$$P_i = 0, \qquad 1 \leq i \leq \ell. \tag{11}$$

وفي كثير من الأحيان تكون بعض النتائج مجرد تكرار أو تبسيط مباشر أو صدى واضح للمعطيات، إلا أن بعض النتائج قد يكون مستغربًا بل ومذهلاً أحيانًا وذلك لكونه كامنا بصورة شديدة التخفي داخل المعطيات. ويلاحظ أن هذه الطريقة لا تتطلب من المستخدم طرح نتيجة يراد إثباتها (وضعها). وفي حالة ما إذا اقترح المستخدم نتيجة معينة لهذا الغرض، فإن هذه النتيجة المقترحة يتم مقارنتها بالنتائج التي يتم الحصول عليها فإن كانت النتيجة المقترحة متضمنة في هذه النتائج، فإنها أي النتيجة المقترحة، تصدق وتثبت بقدر ما تصدق المعطيات وتثبت. أما إذا كانت النتيجة المقترحة غير متضمنة في النتائج فهذا لا يعني بالضرورة نقض أو رفع أو رفض هذه النتيجة برغم صدق المقدمات لأنها – أي المقدمات قد تكون

$$\left(\frac{X\overline{Y}Z}{\overline{Y}}\right) \wedge \left(\frac{XY\overline{W}}{Y}\right) = (XZ) \wedge \left(X\overline{W}\right) = XZ\overline{W}, \qquad (7)$$

في المعادلة (7) استخدمنا مفهوم خارج القسمة البولانية (Boolean quotient)، وهو مفهوم في تسميته تجاوز لأن الجبر البولاني لا يعرف القسمة أصلاً، ولكن تعريفه الرصين يحتاج إلى عملية تقييد (Restriction) مسموح بها، أي أن:

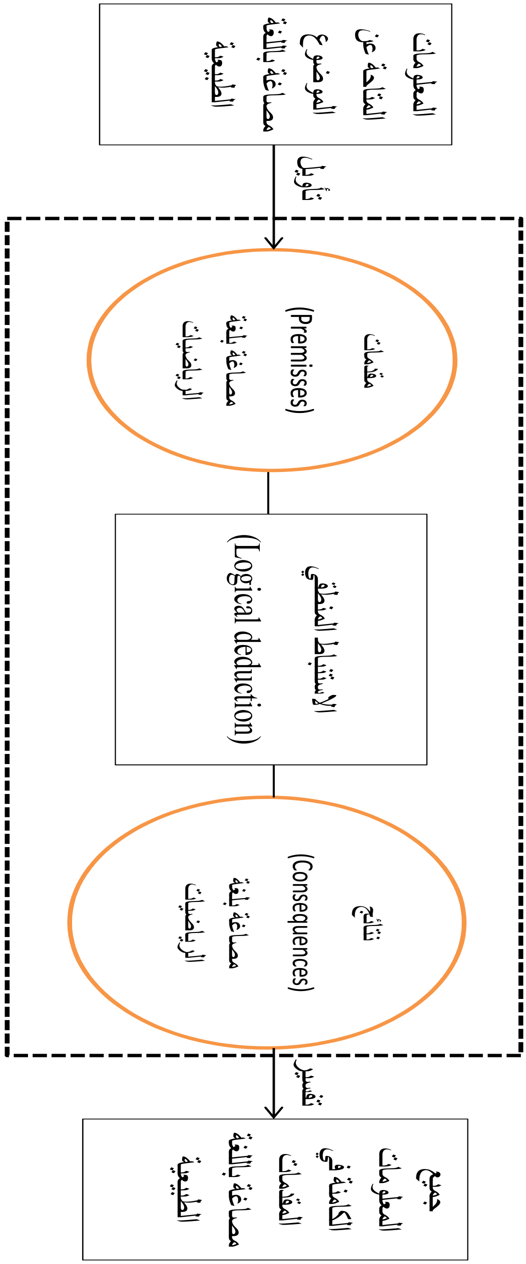
$$\left(\frac{g}{h}\right) = (g)_{h=1}, \qquad (8a)$$

$$\left(\frac{g}{\overline{h}}\right) = (g)_{h=0}, \qquad (8b)$$

يمكننا الآن أن نضيف التراضي بين مضروبين إلى مجموعهما المنطقي دون أن يغير ذلك شيئا، أي دون أن يخل ذلك بقيمة ذلك المجموع، بمعنى أن:

$$X\overline{Y}Z \vee XY\overline{W} = X\overline{Y}Z \vee XY\overline{W} \vee XZ\overline{W}, \qquad (9)$$

ومن ناحية أخرى نلاحظ أن المضروبين XYZ، XYW ليس لهما تراض لعدم وجود تضارب بينهما، وكذلك المضروبان $\overline{X}\,\overline{Y}Z$، XYW ليس لهما تراض لوجود أكثر من تضارب واحد بينهما. ويلخص الشكل رقم (٢) مجموعة الحقائق سالفة الذكر المتعلقة بالتراضي بين مضروبين كما يعطي تمثيلاً تصويريًا لها باستخدام ما يعرف باسم خريطة كارنوه (Karnaugh map) التي يمكن النظر إليها كصورة مطورة من شكل فِنْ (Venn diagram)، كما يمكن اعتبارها جدولاً للصدق مرتبًا في بعدين (two dimensions) بدلاً من بعد واحد، ووفقًا لترميز ثنائي منعكس (reflected binary coding). ويلاحظ أن إعمال عملية الحذف على مجموع المضروبات المعبر عن الدالة f يؤدي إلى تصغير حجم هذا المجموع ويمنع



شكل (١). تصور الانتقال من المقدمات مصاغة باللغة الطبيعية إلى النتائج مصاغة باللغة الطبيعية.

- **الحذف** (Deletion) لمضروب في مجموع المضروبات (Sum-of-products) المعبر عن الدالة f، وذلك نتيجة لامتصاص أو استغراق (Absorption) هذا المضروب في مضروب آخر ينتمي لنفس المجموع، ويحدث ذلك إذا كانت مجموعة حروف المضروب الأول مجموعة جزئية (Subset) من مجموعة حروف المضروب الثاني، فمثلاً المضروب XY يمتص في أي من المضروبات $X\overline{Y}$، X، $\overline{Y}$، 1 حيث 1 ترمز للواحد المنطقي، ومثلاً المضروب $X\overline{Y}Z$ يمتص في المضروب $X\overline{Y}$ وعليه يمكننا أن نكتب

$$X\overline{Y}Z \vee X\overline{Y} = X\overline{Y}, \qquad (6)$$

- **توليد وإضافة التراضي** (Consensus generation and addition) لمضروبين في مجموع المضروبات المعبر عن الدالة f، حيث يوجد التراضي بين مضروبين إذا وجد تعارض واحد بين مجموعة حروف المضروب الأول ومجموعة حروف المضروب الثاني أي إذا وجد متغير واحد ثنائي الصيغة (Biform) في المضروبين بمعنى وجوده بالصورة العادية في أحد المضروبين وبالصورة المعكوسة في الآخر، وفي هذه الحالة يكون تراضي المضروبين هو حاصل الضرب المنطقي لبقية حروف المضروبين مع حذف الحروف المكررة إعمالاً لقاعدة تماثل الفعالية (Idempotency) $\{X \wedge X = X\}$. فمثلا المضروبان $X\overline{Y}Z$ ، $XY\overline{W}$ لهما تراضٍ قيمته $XZ\overline{W}$ نظرًا لوجود تضارب واحد بينهما نتيجة لوجود الحرف المعكوس $\overline{Y}$ في المضروب الأول مع وجود الحرف العادي Y في المضروب الثاني، وقد نتجت قيمة التراضي من الضرب المنطقي:

$$T_i \rightarrow Q_i\,, \qquad (n+1) \leq \mathrm{i} \leq m. \tag{3}$$

فإنها تأخذ الشكل الصفري التالي:

$$T_i\,\overline{Q}_i = 0, \qquad (n+1) \leq \mathrm{i} \leq m. \tag{4}$$

نلاحظ أن العلاقة (3) تمثل الجملة الشرطية (إذا كان T_i كان Q_i) أو مكافئها (Q_i فقط إذا T_i) وهو ما يعني كون الخبر T_i شرطًا كافيًا (Sufficient) للخبر Q_i وكون الخبر Q_i شرطًا ضروريًا (Necessary) للخبر T_i، كما نؤكد أن العلاقة (3) ليست تبديلية بمعنى أنها لا تكافئ العلاقة ($Q_i \rightarrow T_i$)، ولكن إذا اجتمع الشرطان ($T_i \rightarrow Q_i$) و($Q_i \rightarrow T_i$) فإن ذلك يؤدي إلى التكافؤ التام بين الخبرين Q_i و T_i كما في (1).

٢- مجموعة المعطيات تكافئ معادلة واحدة تنشأ من مساواة دالة تبديلية واحدة بالصفر المنطقي وهذه الدالة تنشأ من المجموع المنطقي للصور الصفرية للمعطيات، فمجموعة المعطيات الناتجة من اتحاد مجموعة المعطيات (1) مع مجموعة المعطيات (2) تكافئ:

$$f = \bigvee_{i=1}^{n} (T_i\,\overline{Q}_{\mathrm{i}} \vee \overline{T}_i\, Q_i\,) \;\vee \bigvee_{i=(n+1)}^{m} T_i\,\overline{Q}_i = 0. \tag{5}$$

٣- يتم إعادة كتابة الدالة f الواردة في (5) في صورة مجموع منطقي لجميع ضامناتها الأولية (Prime implicants) وهذه الصورة تعرف باسم المجموع الكامل (Complete sum) كما تعرف باسم صيغة بليك الإسنادية (Blake Canonical Form)[٤٩]. وتوجد طرائق خوارزمية عديدة - يدوية ومحسابية - لتوليد هذا المجموع ومعظمها يعتمد على استخدام تتابع معين لنوعين من العمليات المنطقية[٤٩،٥١]:

كتابه الشهير عن الاستدلال البولاني والمعادلات البولانية[٤٩]. ويمكن للقارئ أيضًا أن يجد وصفًا تفصيليًا لها ولخصائصها وتطبيقاتها في المراجع[٤٨-٥٩]، مع ملاحظة أنها لم تعرف باسمها الحالي إلا مؤخرًا[٥٢-٥٩]، وسوف نعتمد في وصفنا لها على الوصف العربي الوحيد المتاح لها[٥١].

إن الطريقة الاستدلالية الحديثة خوارزمية وليست تجريبية الأسلوب بمعنى أنها تحدد للمستخدم عددًا محدودًا من الخطوات الواضحة يصل به إلى الحل دون الاعتماد على مهارة خاصة أو بصيرة ثاقبة من قبله. وهذه الطريقة تستخدم في طياتها وبصورة ضمنية جميع قواعد الإحلال (Replacement rules) في المنطق[٥١، ٥٤، ٥٥]، كما يمكن إثبات أنها تمثل نوعًا من التوحيد لجميع قواعد الاستدلال (Inference rules) بمعنى أن أية قاعدة من قواعد الاستدلال ما هي إلا حالة خاصة من الحالات التي تتناولها هذه الطريقة[٥١، ٥٤، ٥٥].

ويمكن تلخيص خطوات هذه الطريقة فيما يلي[٥١]:

١- نفترض أن المعطيات أو المقدمات للمسألة محل الدراسة هي في صورة متساويات أو متكافئات منطقية على الشكل التالي:

$$T_i \equiv Q_i \,, \qquad 1 \le i \le n, \tag{1}$$

فنقوم بتحويلها إلى الصورة الصفرية التالية:

$$T_i \, \overline{Q}_i \vee \overline{T}_i \, Q_i = 0\,, \qquad 1 \le i \le n. \tag{2}$$

حيث يرمز الرقم "0" للصفر المنطقي، ويدل الرمز "$\vee$" على المؤثر المنطقي "أو" (OR). أما إذا كانت هذه المعطيات أو بعضها في صورة علاقة احتواء منطقي (Logical inclusion) والتي تسمى أيضًا بعلاقة الضمان المنطقي (Logical implication):

حقيقة ولا يحرك ساكن العلم، وكل دوره هو كشف ما يكون مخفيًا أو مستترًا في المقدمات. ومع هذا التواضع في تحديد هوية الاستنباط ونفعه، نقرر أنه لا بأس باستعماله كوسيلة للاسترشاد لاستكشاف المسائل الغامضة والحرونة، وبصفة خاصة مسألة المعضلات الأخلاقية التي تهمنا هنا. ويصف الشكل رقم (١) خطتنا لهذا الاستكشاف. نلاحظ من الشكل أننا لا نضمن عدالة أو ضبط المصادر التي تمدنا بالمعلومات، وأن خطوة تأويل ما لدينا من المعلومات مصاغة أصلاً باللغة الطبيعية بحيث تصبح مقدمات مصاغة بلغة الرياضيات هي خطوة غير معصومة من كثير من الزلل بسبب المغالطات غير الصورية التي تعتري اللغة الطبيعية. وبدرجة أقل تعاني خطوة تفسير النتائج الرياضية باللغة الطبيعية من مشاكل مماثلة. ولكن قلب عملية الاستنباط يظل عملية رياضية دقيقة تستعمل رموز وأساليب الرياضيات. خلاصة القول، إننا سوف نستعمل هنا أساليب رياضية سليمة للاستنباط، ونجتهد ألا تكون خطوة التأويل السابقة أو خطوة التفسير اللاحقة مفسدة لسلامة عملية الاستنباط بأسرها. كل ما ينفعنا به الاستنباط هو أنه عملية حافظة للصدق (Truth-preserving) فإن كانت مقدماته الرياضية صادقة فإن نتائجه الرياضية تكون صادقة كذلك. ونؤكد أيضًا أن حجم المسألة المنوط بها الاستنباط قد تحدد حاجتنا إلى أو استغنائنا عن الصياغة الرياضية أو الصورية للاستنباط، فإذا كانت المسألة صغيرة الحجم يمكن للعقل البشري (الذكي!) تتبعها في صورتها الكلامية غير الصورية، أما إذا زاد عدد متغيرات المسألة زيادة مفرطة فيتعذر لأي إنسان الاستغناء عن الصياغة الرياضية والحسابات الخوارزمية.

٢. وصف الطريقة الاستدلالية الحديثة

ظهر أول وصف للطريقة الاستدلالية الحديثة (ط دح) في رسالة الدكتوراه التي قدمها بليك (Blake)[٤٨]، ولكنها لم تشتهر حتى قدمها براون (Brown) في

للمنطق الصوري. إن المنطق الصوري يسعى لتقييد اللغة برمزيته المصطنعة المحدودة، وهو يمثل أداة لجعل كثير من الممارسات البشرية (كالطب والهندسة مثلاً) مجردة من العواطف الإنسانية والمناهج العقلانية (Dehumanized and irrational)[٩٠].

٥. المنطق الصوري يرث قصور ونقائص الوصف اللغوي لعملية التشخيص في الهندسة والطب، ومن ثم يجنح إلى التعقيد (Complexity) وعدم الاكتمال (Incompleteness) وعدم الاتصال (Discontinuity)، ولذلك فإنه ليس دائمًا الخيار الأفضل لدعم تشخيص الأعطاب والأمراض[٩١].

٦. إن براهين الصحة (Soundness) والاكتمال (Completeness) لا يمكنها أن تبرر نظامًا للاستنباط برغم أهميتها من الناحية التقنية، لأن هذه البراهين مبنية على الاستدلال الاستنباطي ولأن التبرير الاستنباطي للاستنباط لا يمكن أن يكون مرضيًا لأحد إلا بقدر ما يكون التبرير الاستقرائي للاستقراء[٩٢].

٧. من المشكوك فيه أن ينجح المنطق الصوري في نمذجة أو تصميم نظم البرمجيات عديدة الوكلاء ((Multi-Agent Software (MAS))[٩٣].

٨. المنطق الصوري هو نوع من الفشل ذي المنطقية الزائفة[٩٠].

٩. إن المنطق الصوري لا يتمتع إلا بشيء قليل من الأساس العلمي ومن الفائدة العلمية لأنه لا يستطيع أن يتفادى كثيرًا من المغالطات غير الصورية (Informal fallacies) التي تعاني منها اللغة العادية مثل التجريد (Abstractionism)، والدورانية (Circularity) والاختزالية (Reductionism)، وانتفاء العلاقة (Irrelevance)، والأسباب الكاذبة (False causes)، والتبسيط (Simplification)[٩٠].

ويتحدث بعض العلماء المعاصرين عما يسمونه تجاوزًا وتهكمًا بفضيحة أو عار الاستنباط (The scandal of deduction)[٩٤، ٩٥]، فالاستنباط لا يأتي بجديد

١. " *اعلم أن المنطق اليوناني لا يحتاج إليه الذكي ولا ينتفع منه البليد*"[٨٦]، هذه مقولة شهيرة لشيخ الإسلام ابن تيمية رحمه الله تعالى، فضلاً عن أن له كتابين شهيرين في نقض المنطق[٨٧] والرد على المنطقيين[٨٨]. والمنطق اليوناني الذي ذمه شيخ الإسلام هو نوع المنطق الاستنباطي الذي كان سائدًا في عصره. ولكن شيخ الإسلام كان يستعمل نوعًا من المنطق المنضبط إسلاميًا، وهو يعتبر في الحقيقة أول مؤسس لما يعرف الآن باسم المنطق الاستقرائي (Inductive logic).

٢. " *من تمنطق فقد تزندق*"، هذه مقولة أخرى لشيخ الإسلام رحمه الله تعالى قالها لأن المنطق في عصره كان خادمًا طيعًا للفلسفة، ولم يكن اكتسب الحيادية التي يتمتع بها حاليًا بعد أن أصبح فرعًا من الرياضيات. إشكالية ارتباط المنطق بالفلسفة أن الفلسفة عند الزنادقة أو الملاحدة تضاد الدين وسيلة وغاية، وهي عند المؤمنين تخالف الدين وسيلة ومنهجًا وإن كانت تؤازره قصدًا وغاية. وهذه المخالفة المنهجية (methodological) في الحالتين كلتيهما مصدر للبلبلة والشك وعدم اليقين. ولا يصح بحال فرض مقدمات منطقية في العقائد والإلهيات لأن ذلك يخالف توحيد الأسماء والصفات. وخلاصة القول ضرورة قصر استعمالات المنطق على أمور دنيوية قد ينفع فيها[٥١].

٣. المنطق الصوري يتضمن نزعة إلى التسامي والاستعلاء (Transcendence) لا تناسب دراسة المحاجة (Argumentation) لأن المحاجة لا تقع في مجال رؤية المنطق[٨٩]، وربما لأن المنطق يريد حسمًا محددًا للحقائق، بينما المحاجة تعني التخلي المسبق عن أي التزام، والاستعداد (ظاهريًا على الأقل) للنزول على الرأي المخالف إذا انتصرت حجته.

٤. المنطق الصوري هو إساءة لاستخدام (Misuse of) اللغة العادية. فالأولوية المعرفية (Epistemological primacy) هي للغة الطبيعية وليست

فهل هي ربا محرم أم هي رسوم إدارية؟ كما سيحدث خلاف في حال التيقن من كون الفوائد ربا حول هل الضرورة متحققة فعلاً بحيث تبيح محظور أخذ هذا القرض الربوي؟ وقد يحدث خلاف آخر حول هل الأولى هو حل مشكلة الإفلاس بالاقتراض أم بالاندماج والاتحاد مع شركات أخرى؟

١,٣. حول الاستنباط المنطقي

ثمة جدل عنيف في الأوساط العلمية حديثًا وقديمًا حول فائدة ونفع المنطق الصوري (Formal logic) المستعمل في الاستنباط المنطقي (Logic deduction). فثمة من يذكر له منافع في تقوية التفكير الناقد أو المنطقي عند مستخدميه[٨٤، ٨٥]. وقد بلغ الإعجاب بالمنطق الاستنباطي عند العالم الكبير ليبنيز (Leibniz) حد الإفراط والغلو حيث ذهب إلى أن القياس المنطقي (Syllogism) هو واحد من أجمل وأبرز ما تفتق عنه العقل البشري:

"I hold the invention of the syllogistic form to be one of the most beautiful inventions of the human mind, and indeed one of the most notable."

وقد أبدى ليبنيز رأيه هذا رغم أنه نفسه مشترك مع نيوتن (Newton) في ابتكار علم التفاضل والتكامل (Calculus)، وهو فرع الرياضيات الذي لعب الدور الأكبر في ترييض العلوم كلها أي في إسباغ صبغة الرياضيات عليها (Mathematization of all sciences)، وكان الأولى بالعالم ليبنيز (من وجهة نظر شخصية على الأقل) أن يزعم أن التفاضل لا القياس هو الأعظم بين مبتكرات البشر. ومثل هذا الإعجاب المفرط بالمنطق عند أنصاره كان مجاوزًا للحد بطبيعة الحال وتسبب في ردة فعل عنيفة ضده، نلخص فيما يلي عددًا من الأقوال المهمة المعارضة للمنطق الصوري:

التي يتعرض لها ويحتاج لاتخاذ قرار فيها. ولكن الصعوبة تبرز في أن مبدأين أو أكثر من المبادئ الأخلاقية التي يمكن تطبيقها على هذه المشكلة قد يكون بينهما تعارض، أو أن مبدأ أخلاقيًا واحدًا ينطبق على هذه المشكلة ولكنه قد يؤدي إلى قرارين مختلفين بسبب الاختلاف في الفهم أو التفسير. فعلى سبيل المثال، قد يواجه المهندس الذي يعمل لدى شركة مشرفًا على تشييد برجٍ في مدينة مشكلة في أنه قد علم بأن شركته قد استخدمت تصاميم بها أخطاء حسابية إن لم تصحح فقد تؤدي إلى وقوع خسائر مادية وبشرية لسكان المدينة. وقد قام المهندس بواجبه الأخلاقي فنبه مدير الشركة عن هذا الخلل، إلا أن المدير طلب منه أن يغض الطرف وأن يواصل المشروع وكأن خطأ لم يكن. فالمهندس لديه مبدأ أخلاقي يطلب منه الحفاظ على أنفس وأموال سكان المدينة، ولكنه إن طبقه سيفضح تصاميم الشركة الخاطئة للمسؤولين وقد يدمر مستقبلها، ولديه مبدأ أخلاقي آخر يطبق على مشكلته يطلب منه أن يحافظ على أسرار العمل وعدم هتك حقوق الملكية الفكرية لدى الشركة التي يعمل بها. فأي المبدأين الأخلاقيين يطبقه؟ ولماذا؟

ج- مشاكل الخلاف (Problems of Disagreement):

تحدث هذه المشاكل عندما يختلف أولو الرأي والنظر من الأفراد أو المجموعات حول تفسير وتطبيق وموازنة الأولويات للمبادئ الأخلاقية في حالات معينة. وتزداد درجة الخلاف ويصبح أكثر تعقيدًا داخل الشركات الهندسية التي لابد للأفراد أن يعملوا فيها معًا في إطار علاقات هيكلة السلطة والصلاحيات. على سبيل المثال، عندما تواجه شركة هندسية مشكلة الإفلاس فإنها قد تضطر للبحث عن مصدر للتمويل فتأخذ قرضًا بفوائد لسد العجز وحل مشكلتها، فهنا سيحدث اختلاف بين أولي الرأي والنظر في الشركة حول تفسير طبيعة هذه الفوائد

١٠. تنص مواثيق أعراف كثير من الجمعيات المهنية الهندسية على أنه لا يجوز للمهندس التعليق على مدى الكفاية المهنية لزملائه المهندسين. طالب مدير إحدى الشركات مهندسًا مرؤوسًا له بعمل تقويم مهني لمهندس متقدم للعمل بنفس الشركة، فهل يعتبر الإدلاء بما يعرفه عن ذلك المتقدم انتهاكًا للأعراف الأخلاقية الهندسية؟

من الأمثلة السابقة يتضح أن المعضلات تنشأ عندما يحدث تعارض بين اثنين أو أكثر من الالتزامات الأخلاقية أو الواجبات أو الحقوق أو المنتجات أو الأفكار، ويبدو أنه من غير الممكن مراعاتها جميعًا بالكامل، إذ يلزم حينئذ تقديم الأهم منها على المهم. يوجد – على الأقل– ثلاثة أنواع من التعقيدات، إن وجدت في حالات ما فإنها تسبب المعضلات الأخلاقية وهي: مشاكل الإبهام، ومشاكل الأسباب المتعارضة، ومشاكل الخلاف، وفيما يلي بيان لكلٍ منها[١٢-١٧]، مع إيضاحات مأخوذة من مجال ممارسة مهنة الهندسة.

أ– مشاكل الإبهام (Problems of Vagueness):

عند حدوث معضلة ما، قد يواجه الإنسان مشكلة عدم القدرة على تحديد أي المبادئ أو الاعتبارات الأخلاقية أجدر بالتطبيق وأحق بالتقديم. فعلى سبيل المثال، هناك دائمًا غموض كبير حول طبيعة "الهدية" المقدمة لمهندس من شركة تتعامل مع شركته، وهل يمكن فعليًا اعتبارها هدية رمزيَّة وأمرًا مقبولاً لا ضير منه ولا غبار عليه، أم أنها في واقع الأمر لا تعدو أن تكون سوى رشوة مستترة غير مقبولة.

ب– مشاكل الأسباب المتعارضة (Problems of Conflicting Reasons):

في هذا النوع من المعضلات – وهو الأكثر حدوثًا ووقوعًا– يكون واضحًا تمامًا لدى المرء أي المبادئ أو الاعتبارات الأخلاقية يمكن تطبيقها على المشكلة

يسمح للطلاب بأخذها معهم، كما أنه يحرص على ألا يجيب على هذه الأسئلة حتى وإن سئل عنها صراحة. هل يمثل هذا إخلالاً بالعدالة وإهدارًا لوظيفة الامتحان كأداة للتقويم الصحيح للطلاب؟

٦. هل يتحمل مصمم آلة قاطعة كالمخرطة أو المنشار الكهربائي المسؤولية إذا استخدم شخص هذه الآلة بصورة خاطئة أدت إلى بتر أصابعه؟

٧. يجب تأريض الأجهزة الكهربائية التي تستعمل جهودًا كهربائية عالية لتفادي تفريغها للشحنات المتراكمة خلال أجساد مستخدميها من البشر. يقوم الناس بإزالة الخط الأرضي من قوابس هذه الأجهزة الكهربائية لتلائم مقابس (منابع) الكهرباء لهم. ما هي المسؤولية الأخلاقية لمن يزيل الخط الأرضي من القابس إذا تسبب في الصعق الكهربائي لإنسان؟

٨. يوجد في الأسواق مذيبات قوية جدًا (يتشكل معظمها من حمض الكبريتيك المركز) يمكن استعمالها لتسليك البلاعات المسدودة بتذويب ما فيها من دهون متصلبة. يمثل استعمال هذه المذيبات خطورة شديدة، ولذلك تكتب تحذيرات تفصيلية على الزجاجات الحاوية لها. وبرغم أن هذه التحذيرات تكتب باللون الأحمر، فإنها تكتب بإسهاب واستفاضة شديدين قد يؤديان إلى ضجر القارئ، كما تكتب بخط صغير يتعذر تمييزه على الكثيرين. هل أبرأت الشركة المصنعة للمذيبات ذمتها بكتابة مثل هذه التحذيرات؟

٩. من وجهة نظر الإحصاء، توجد فروق إحصائية مهمة (Significant statistical differences) تثبت أن تدخين السجائر يؤدي إلى الإصابة بمرض سرطان الرئة المفضي إلى الموت. تقوم شركات السجائر بكتابة تحذير على علب السجائر تنوه فيه بخطرها على صحة الإنسان، فهل أبرأت الشركات ذمتها بهذا التحذير؟ وما مدى مسؤولية من يساهم في تيسير وصول السجائر إلى المستهلك؟

١,٢. حول المعضلات الأخلاقية

المعضلات الأخلاقية هي مشاكل مستغلقة لا يهتدى بسهولة إلى حلول مقبولة لها من الناحية الأخلاقية، وكما أسلفنا القول فإنها من أبرز أنواع المسائل الحرونة. تحفل أدبيات الموضوع بأمثلة كثيرة للمعضلات الأخلاقية[٦،٧]، وفيما يلي بعض الأمثلة الشائعة:

١. هل يجوز للجراح أن يشرع في إجراء جراحة لمريض يغلب على الظن أنها قد تفضي إلى وفاة المريض؟ وإذا كان احتمال وفاة المريض عند إجراء العملية هو ل١، وكان احتمال وفاته بدون العملية هو ل٢، فما هو الحد الفاصل في العلاقة بين الاحتمالين ل١ و ل٢ الذي يتقرر عنده إجراء العملية الجراحية؟

٢. هل يجوز لطالب أن ينتفع بأوراق كتب فيها أستاذه نسخة أولية لأسئلة الامتحان، علمًا بأن الطالب عثر على هذه الأوراق دون قصد من جانبه، وإنما بسبب إهمال الأستاذ الذي ترك الأوراق على الطاولة في قاعة الدرس؟

٣. تضاف بعض المواد الحافظة إلى الأطعمة لتمديد فترة صلاحيتها، ولكن ثبت أن هذه المواد تسبب السرطان في حيوانات التجارب فهل يُسمح بالاستمرار في استخدامها في الطعام الذي يستخدمه البشر؟

٤. هل يجوز لمدير في إحدى الشركات نما إلى علمه نية الشركة إلى تسريح بعض مرؤوسيه أن يخبر هؤلاء المرؤوسين بمعلوماته قبل الإبلاغ الرسمي لهم بشهر، وأن يسمح لهم بصرف أوقات العمل للبحث عن وظائف جديدة لدى شركات أخرى؟

٥. أستاذ جامعي يحتفظ بخمس نماذج لأسئلة الامتحان في المقرر الذي يدرسه، وهو يستعمل واحدًا منها بصورة عشوائية في كل فصل دراسي. وحرصًا على ألا يتداول الطلاب الأسئلة في الفصول التالية يحتفظ بأوراق الأسئلة ولا

- كل مسألة حرونة تمثل مظهرًا أو عرضًا (Symptom) لمسألة حرونة أخرى.

- يمكن تفسير مسببات (Causes) المشكلة أو المسألة الحرونة بطرائق عديدة، ويؤدي اختيار تفسير معين إلى تحديد طبيعة الأسلوب الملائم للحل.

- لا مجال للخطأ عند التعامل مع المشاكل والمسائل الحرونة، إذ بينما تسمح المسائل الوديعة بوضع الفرضيات ثم نقضها بهدف الوصول إلى الحقيقة، فإن التعامل مع المشاكل والمسائل الحرونة يتطلب تنفيذ حل يهدف إلى تحسين خصائص العالم الذي نعيش فيه، ولذلك يتحمل القائمون بحل المشاكل والمسائل الحرونة المسؤولية عن كافة الإجراءات التي ينجزها الحل والتي قد تكون ضارة وغير معكوسة[٤٧].

وأهم وأشهر المسائل الحرونة هي مسائل في الإدارة أو التخطيط بعيد المدى (Long-term planning)، وكثير من مسائل التصميم الهندسي (Engineering design)، فضلاً عن المسائل التي تهمنا هنا وهي مسائل المعضلات الأخلاقية. وقد بلغ الشبه بين مسائل التصميم الهندسي والمعضلات الأخلاقية حدا دعا إلى استخدام مسألة التصميم الهندسي كوسيلة لنمذجة المعضلات الأخلاقية[٨٣].

إن أهم قاعدة للتعامل مع المسائل الحرونة هي أنها يجب ألا تعامل معاملة المسائل الوديعة، بل يجب محاولة التعرف عليها أولاً تمهيدًا لتذليلها وتطويعها، فإن لم يتسن ذلك لزم العمل على إعادة تهيئة وتعديل وتكييف الشروط والأحوال الحاكمة لهذه المسائل. الأسلوب الأمثل للتعامل مع المسائل الحرونة هو مناقشتها بالتفصيل مع كافة المعنيين بها، والتوصل إلى نوع من التراضي والتوافق بين الجميع من خلال طرح كل البدائل المتصورة لفهم المشكلة ومن خلال معرفة المصالح والأولويات والقيود المتضاربة والمتنافسة.

حرونة أخرى. ولذلك ينصح بالتوقف عندما تنضب الموارد المخصصة للحل، أو عند التوصل لنتيجة تبدو ظاهريًا أو يمكن جزافًا اعتبارها جيدة بما فيه الكفاية، أو عندما يشعر القائمون بالحل بعجزهم عن أن يأتوا بجديد مفيد.

- حلول المسألة الحرونة لا توصف بأنها صحيحة أو خاطئة، بل تقوَم ويقارن بينها بوصف بعضها بأنه أفضل أو أسوأ من البعض الآخر، ومثل هذا التقويم يفتقر إلى الموضوعية إذ يعتمد كثيرا على شخصية القائم به ومصالحه الخاصة ومنظومة القيم لديه وانتماءاته الفكرية وما إلى ذلك.

- يتعذر اختبار الحلول المقترحة للمسألة الحرونة عاجلاً أو آجلاً، إذ لا تعرف نتائج وعواقب أي حل إلا بعد تنفيذه فعلاً.

- أي حل للمسألة الحرونة هو عملية متفردة قائمة بذاتها، حيث لا يمكن اختبار الحل بالتجربة والخطأ (Trial and error) لأن عواقب أي حل غير معكوسة (Irreversible)، بل إن أية محاولة لتعديل الحل بعد تنفيذه أو لتصحيح عواقبه غير المرغوبة تولد مجموعة جديدة من المسائل الحرونة.

- ليس للمسألة الحرونة مجموعة من الحلول الممكنة يمكن تعدادها أو سردها بصورة مستنفدة، حيث لا يوجد معيار معين يحدد نهاية لهذا التعداد، ومن الوارد عدم التوصل إلى أي حل على الإطلاق بسبب التناقضات المنطقية في الصورة المطروحة للمسألة.

- كل مسألة حرونة وحيدة في بابها وفريدة في نوعها، فليس ثمة طوائف من المسائل أو المشاكل الحرونة تتشابه عناصرها بحيث يمكن حلها جميعها بأسلوب مماثل أو باستخدام نفس المبادئ.

- المسألة الوديعة تتوقف معالجتها عند نقطة توقف محددة يتضح عندها تمام التوصل إلى حل للمسألة.

- يمكن تقويم أي حل مقترح للمسألة الوديعة باعتباره حلاً صحيحًا أو خاطئًا.

- قد تكون المسألة الوديعة معقدة (Complex)، ولكنها تقبل التحليل والحل بالطرائق التنقيبية المعروفة خلال زمن مقبول، ويدخل ضمن ذلك المسائل غير القابلة للتتبع التي تتطلب خوارزميات حلها زمنًا أسيًا، ولكن يمكن حلها تقريبيًا بواسطة خوارزميات أو إجراءات تنقيبية سريعة.

- أية مسألة وديعة تنتمي إلى طائفة من المسائل أو المشاكل الشبيهة التي يمكن حلها جميعها بأسلوب مماثل.

- المسألة الوديعة لها حلول يمكن تجربتها والعدول عنها إن اقتضى الأمر بدون خسائر تذكر[٤٧].

أما المسائل الحرونة فهي مسائل سيئة التعريف (Ill defined). تتسم بالإبهام (Ambiguity) وتفتقر إلى الحد الأدنى من التراضي أو التوافق (Consensus) بين المعنيين بها على تحديد ماهيتها فضلا عن اختيار الأسلوب المناسب لحلها، ومن ثم فهي تعاني من كثرة الآراء المتباعدة (Divergent opinions) حول وسائل حلها. توجد عشرة معايير يتم عادة التعرف بها على المسألة الشريرة أو الحرونة[٤٧]:

- لا توجد صياغة محددة للمسألة الحرونة، ويتعذر إعطاء وصف تفصيلي لها ما لم يسبق ذلك محاولة للسرد المستنفد لكافة الحلول الممكن تصورها لها.

- لا تتمتع المسألة الحرونة بقاعدة للتوقف، حيث لا يتم إطلاقًا بلوغ حل نهائي أو كامل أو تام الصحة، بل تتطور المسألة باستمرار وتتبثق عنها مسائل

ما يمكن استنتاجه منها في أبسط صورة ممكنة. الخطوة الأهم في هذه الطريقة هي خطوة حساب المجموع الكامل لدالة تبديلية (Switching) أو بولانية (Boolean)[٤٨، ٦٠-٧٧]. وإذا تم إضافة مقدمات جديدة للمقدمات الأصلية، فإنه لا يتم حساب المجموع الكامل من البداية، إذ ثمة صورة تزايدية (Incremental) للطريقة تستفيد من المجموع الكامل الأصلي، وتبذل أقل جهد ممكن لتعديله إلى مجموع جديد[٥٨، ٧٨- ٨٢].

تم تنظيم البحث على النحو التالي: نتحدث عن المسائل الحرونة في الفصل الفرعي ١,١ كما نقدم وصفًا للمعضلات الأخلاقية في الفصل الفرعي ١,٢، ونشير إلى الجدل الكبير حول المنطق الصوري أو الاستنباط المنطقي في الفصل الفرعي ١,٣. نخصص الفصلين الثاني والثالث لوصف الطريقة الاستدلالية الحديثة وبيان خصائصها. نقدم في الفصل الرابع مدارسة لثلاث معضلات أخلاقية شهيرة. نختتم الورقة بتعليق وخاتمة في الفصل الخامس.

١,١. حول المسائل الحرونة

إن مصطلح "المسائل الحرونة" أو "المسائل الشريرة" (Wicked problems)[٤٥- ٤٧] يبرز الفروق الفاصلة بين هذه الطائفة من المسائل وطائفة المسائل التقليدية المسماة بالمسائل الوديعة أو المذللة أو المروضة أو الخيرة (Tame or righteous problems). ويمكن فهم الاختلاف بين هذين النوعين من المسائل بملاحظة أن المسألة أو المشكلة الوديعة تتميز عن نظيرتها الشريرة بأنها تتمتع بالخصائص التالية[٤٧]:

- المسألة الوديعة لها تعريف مستقر حسن الصياغة.

نلاحظ أولاً أن مسائل المعضلات الأخلاقية لا تندرج تحت طائفة المسائل حسنة الصياغة (Well-posed problems) التي يمكن حلها بالخوارزميات (Algorithms)، ولا حتى تحت طائفة المسائل المبهمة التي يتم التعامل معها باستخدام الإجراءات التجريبية أو التنقيبية أو الاستكشافية (Heuristics) وإنما تندرج تحت نوع أصعب كثيرًا من المسائل التي تسمى المسائل الحرونة أو الشريرة (Wicked)، وهذه مسائل لا توجد أساليب (Techniques) أو مقاربات (Approaches) للتعامل معها[٤٥- ٤٧].

من المتفق عليه أنَّ ثِمة منطق للاستدلال الأخلاقي (Ethical reasoning) له نفس البنية التي تتمتع بها صنوف الاستدلال الأخرى مثل الاستدلال الرياضي والعلمي والطبي والهندسي[١٣]. فالاستدلال عمومًا يبدأ بهدف ومبادئ ووجهة نظر حاكمة تفرض نوعا من الافتراضات (Assumptions) التي يمكن أن نسميها مقدمات (Premises) وهذه تؤدي إلى مُتضمَّنات (Implications) أو نتائج (Consequences). إن الانتقال من المقدمات إلى نتائج يتم ذهنيًا في وعاء اللغة الطبيعية وهو ما نسميه بالاستنباط غير الصوري (Informal deduction)، ولكنه يمكن أن يتم أيضا بشكل أكثر إحكاما في وعاء الرياضيات، وهذا ما نسميه بالاستنباط الصوري (Formal deduction).

نقترح هنا استخدام الاستنباط المنطقي كوسيلة استكشافية لمسائل المعضلات الأخلاقية، حيث نقوم بتدارس سيناريوهات مختلفة أو مقدمات مختلفة تصف معضلة أخلاقية معينة من وجهات نظر متباينة. تتم الاستفادة من النتائج المختلفة التي يتم الحصول عليها في تفهم المعضلة والتعامل معها تحت ظروف مختلفة.

نقدم هنا طريقة قوية للاستنباط في المنطق الإخباري تسمى الطريقة الاستدلالية الحديثة[٤٨- ٥٩]. تستخلص هذه الطريقة من مجموعة من المقدمات كل

الكفاية هي خوارزمية بليك– تايسون المحسنة. وللطريقة الاستدلالية الحديثة صورة تزايدية تضيف إلى مجموعة المقدمات الأصلية بعض المقدمات الجديدة، ثم تسعى لإيجاد النواتج المجددة تزايديًا أي بدون الحاجة إلى إعادة حساب المجموع الكامل من البداية. نوظف هذه الطريقة في تدارس سيناريوهات مختلفة أو مقدمات مختلفة تصف معضلة أخلاقية معينة من وجهات نظرية متباينة. تفيد المقارنة بين نتائج هذه السيناريوهات في التوصل لحلول مقبولة لعدد من المعضلات المهمة من بينها معضلة اضطرار المرء لدفع رشوة للحصول على حقه، ومعضلة الاستهلاك الآدمي للأغذية المعدّلة وراثيًا ومعضلة التخلص من مادة غذائية بأكملها إذا لحق بعضها نجاسة. العمل المقدم في هذه الورقة هو تمهيد أولي لبناء حزمة برمجية للمعاونة في حل المعضلات مع استخدام مقدمات منضبطة بأصول وقواعد الفقه الإسلامي في صور حتمية أو في صور تخص المنطق الضبابي أو المنطق الضبابي الحدسي.

الكلمات الدالة: المعضلات الأخلاقية، الاستنباط، المنطق الإخباري، الطريقة الاستدلالية الحديثة، وجهات النظر المتباينة.

١. المقدمة

تقنين وسائل رياضية للتعامل مع المعضلات الأخلاقية الهندسية، وهي المشاكل الصعبة التي لا يتيسر الوصول إلى حل لها يكون مقبولاً من الناحية الأخلاقية. وهذه المعضلات صارت ظاهرة مهمة في الحياة المهنية الحديثة[١-٤]، وصارت دراستها ركيزة أساسية في فهم أخلاقيات المهنة أو العمل[٥-١٩]، كما أصبح من الضروري التعامل معها لأجل تناولها من منظور إسلامي[٢٠-٤٤].

مجلة جامعة الملك عبدالعزيز: علوم الحاسبات وتقنية المعلومات، م٣، صفحة ٧٣-١٢٧ (٢٠١٤م/١٤٣٦هـ)
DOI: 10.4197 / Comp. 3 -1.3

توظيف الطريقة الاستدلالية الحديثة في استكشاف الجوانب الخفية في المعضلات الأخلاقية الهندسية

علي محمد رشدي وطالب منصور الشهري
ومحمد محسن الزروان ومحمد علي رشدي*

قسم الهندسة الكهربائية وهندسة الحاسبات، كلية الهندسة،
جامعة الملك عبدالعزيز، جدة، *المملكة العربية السعودية*
* *قسم الهندسة الطبية وهندسة النظم، كلية الهندسة*، جامعة *القاهرة*،
الجيزة، جمهورية *مصر العربية*
arushdi@kau.edu.sa

المستخلص. تنشأ المعضلات الأخلاقية كمشكلات يصعب حلها لا لنقص في القواعد والمبادئ الأخلاقية التي يمكن الرجوع إليها وإنما لأسباب أهمها الإبهام وتعارض المصالح والخلاف على الأولويات. تقترح ورقة البحث الاستعانة بالاستنباط المنطقي في استكشاف الجوانب الخفية في المعضلات الأخلاقية الهندسية مما قد يعين على حلها. تقدم الورقة طريقة قوية للاستنباط في المنطق الإخباري تسمى الطريقة الاستدلالية الحديثة. تستخلص هذه الطريقة من مجموعة من المقدمات كل ما يمكن استنتاجه منها في أبسط صورة ممكنة. تقوم هذه الطريقة بصياغة مجموعة المقدمات في صورة دالة تبديلية واحدة مساوية للصفر، ثم تحسب المجموع الكامل لهذه الدالة كاتحاد لكل النواتج الأولية، حيث يتم اشتقاق المجموع الكامل بطريقة عالية

(القســم العربي)

المحتويات

﴿ القسم العربي ﴾

﴿ القسم الإنجليزي ﴾

■ سعر النسخة ■

- داخل المملكة ١٠ ريالات سعودية
- خارج المملكة ١٠ دولارات أمريكية

■ البيع والاشتراك ■

مركز النشر العلمي – جامعة الملك عبدالعزيز
ص.ب. ٨٠٢٠٠- جدة ٢١٥٨٩- المملكة العربية السعودية

■ التبادل ■

عمادة شئون المكتبات – جامعة الملك عبدالعزيز
ص.ب. ٨٠٢١٣- جدة ٢١٥٨٩- المملكة العربية السعودية

مطابع جامعة الملك عبدالعزيز

مجلة جامعة الملك عبدالعزيز: علوم الحاسبات وتقنية المعلومات، م٣، ١٢٨ صفحة (٢٠١٤م/١٤٣٦هـ)
ردمد ٦٣٣٦-١٦٥٨
رقم الإيداع ١٤٣٤/١٠٢٨

مجلة
جامعة الملك عبد العزيز
علوم الحاسبات وتقنية المعلومات

المجلد ٣
٢٠١٤ م
١٤٣٦ هـ

مركز النشر العلمي
جامعة الملك عبد العزيز
ص.ب. ٨٠٢٠٠- جدة ٢١٥٨٩
http://spc.kau.edu.sa

الله

بسم الله الرحمن الرحيم