UNIVERSITÀ DEGLI STUDI MEDITERRANEA
DI REGGIO CALABRIA

Dipartimento di Giurisprudenza, Economia e Scienze Umane

Scuola di Dottorato di Ricerca in Diritto ed Economia
Curricula Economia e metodi quantitativi
XXXV Ciclo

TESI DI DOTTORATO

The complexity of Decisions mechanism design: Decision Support Tools.

Settore scientifico:
SECS-P/06 ECONOMIA APPLICATA

Coordinatore:
Prof. Attilio Gorassini

Tutor:
Prof. Bruno Antonio Pansera

Dottoranda:
Merenda Domenica Stefania

Anno accademico 2021-2022

INDEX

Introduction

The individual finds himself having to make continuous decisions without knowing the relative consequences with precision, in which the subjects are faced with different opportunities of choice. These are situations characterized by uncertainty.

To overcome uncertainty, over the years we have tried to formulate well-defined rules that would allow us to study a decision-making problem in a rational way. No.n time the identification of the rules has been influenced by two interpretations: the normative and the descriptive one. The first, theoretically analyzing the behaviors of a perfectly rational ideal person, tends to identify them as abstract canonical norms; the second instead, starting from the observation "in the field" of the subjects, tends to identify them with the behavior of real and "reasonably" rational people.

Subsequent interpretations of these aspects have led to the introduction of a new vision of "irrational" individuals with the consequent proposal of new methodologies for the analysis of choices.

In this way, the problem of how to choose among the available alternatives emerges, using information of a heterogeneous nature that makes it possible to make the elements connected to the decision-making problem “legible”.

The aim of the work is to illustrate the characteristics of the different tools to seek an integrated approach in order to reach the best possible decision.

The paper consists of six chapters. In the first chapter, the concept of complexity of deciding is examined, a reflection is also made about the current situation of the Covid-19 pandemic which has brought the complexity of decisions to a high level. The second chapter is dedicated to

the concepts of artificial intelligence, with the different types of learning. The decisions taken with fuzzy logic represent a relevant environment in the choice problems characterized by uncertain and incomplete information, analyzed in the third chapter. These latter elements represent the tools used in the fourth chapter to create a hybrid model of fuzzy logic and artificial neural networks. The last two chapters dealt with the research line of Multicriteria Decision Analysis.

In the appendix, an interesting research on RSA public key cryptography is proposed, useful in terms of information security that represent an element of fundamental importance in the decision-making process.

1 Chapter: the art of deciding and its complexity

1.1 The art of deciding; 1.2 Theoretical conceptualizations of the decision; 1.3 Decision support systems; 1.4 The complexity of deciding; 1.5 Decision is knowledge; 1.6 The Complexity of "Deciding" at the time of Covid-19: Some Thematic Reflections.

1.1 The art of deciding

In the real context, there is an essential activity that each individual has to perform in every sector: reference is made to the so-called art of deciding. The decision-making activity involves a certain degree of responsibility and a certain level of ever-increasing risks due to the increasing complexity of the systems.

This complexity can be determined by the presence of multiple alternatives and by the dense connections existing between the elements of the decision-making process.

In the prefigured context, the role of the decision maker becomes increasingly difficult, so much so that different methods and quantitative models are sought to support extremely complex processes. Among these, the tools to support the decision maker emerge.

Regarding the art of decision making, many theorists have contributed to the development of the pivotal discipline which is the theory of decisions, finding wide interest among mathematicians, economists, statisticians, philosophers, logicians, psychologists and so on.

Decision theory can be considered as a result of the contributions of different disciplinary studies aimed at analyzing the activity of individuals to make decisions. The origins of this theory date back to the early 1900s with keen interest from the logical, mathematical and managerial fields. It is interesting to underline that the first application area was the military sector.

The concept of deciding can be identified as the activity of identifying the most favorable alternative among the possible options, implemented through a precise valuation method.

The decision-making activity is characterized by the presence of essential components: the definition of a set of alternatives and therefore of a set of actions that can solve the decision-making problem; the presence of expectations understood as possible outcomes related to the options.

The decision-making literature has focused attention on three characterizing aspects: on the one who takes the decision, on the method in which the decision-making process is carried out and on the result.

On the basis of this perspective, it is found that in relation to the subject defined as the decision maker, the type of perspective is subjective and on the basis of the main scientific findings a difference is made between individual decisions (decisions implemented by the individual decision maker or implemented by an organization in the case in which it concerns the achievement of a common goal) and group decisions (characterized by strong complexity and taken by the group itself, by an individual for the

group - leader, by another group according to the logic of dominance). In relation to the method, the type of perspective is procedural and in this context scientific research has focused on the attitude and behavior of the decision maker according to an examination of the concept of rationality[1]. The third aspect concerns the object of the investigation, that is the decision, where the type of perspective is precise or objective, with respect to which the scientific interest has investigated the main distinctions between structured and unstructured, planned and unscheduled decisions.

The main authors who examined the taxonomies just mentioned are: Keen & Morton for structured decisions (they occur frequently, are characterized by a short time horizon and present detailed information) compared to unstructured ones (where the time horizon longer, the information is not perfectly available and there are subjective elements that influence the decision); Simon with reference to planned decisions (they have the character of repetition and occur with a precise frequency such as to allow the structuring of a well-defined standard procedure) and unscheduled (non-recurring therefore it is necessary to develop specific decision-making procedures that are more complex).

Central element of decision theories is the so-called decision-making process which represents the set of multiple tasks and functions that are implemented to solve a complex problem.

---

[1] Rational behavior involves pursuing one's goals in accordance with a predefined set of preferences and priorities. Agnoli, P., & Piccolo, F. (2008). *Probabilità e scelte razionali: una introduzione alla scienza delle decisioni*. Armando editore. The figure of the homo oeconomicus is defined, that is, the fully or perfectly rational economic agent.

On the basis of the theoretical approach, this process is configured as a series of sequential phases to be put in place by the decision maker/agent in order to concretely take a decision. these phases are: the definition of the problem, in this regard the differences between structured and unstructured decision problems, between planned and unplanned decision problems have been examined; the definition of the objective, a fundamental phase that must respect certain characteristics identified by the acronym SMART (Specific, Measurable, Achievable, Relevant, Time-based); the collection of information, at this stage it is essential to carry out a careful analysis to identify those information that are relevant for making the decision; identification of possible options, on the basis of available resources and existing constraints, all possible alternatives are identified; the evaluation of the alternatives, which consists in carrying out a careful analysis of all the costs, all the benefits, all the positive and negative elements of each alternative; the choice of the alternative; the decision maker identifies the option that guarantees the best result; and evaluation of results; the consequences determined by the choice made occur, in case of negative effects the decision maker must repeat the entire analysis, in case of positive results the process is considered concluded.

The first current of decision-making research is called "*classical decision theory*", which is mainly based on the perspective of absolute rationality, on linearly structured decision-making and on instant decision. This scientific approach is mainly based on the studies of Von Norman and Morgenstern on the perfect rationality of the decision maker who enjoys the ability to reach the optimal choice; the same authors introduce *"Game Theory"* and "*theory of maximization of expected utility*", Savage's idea of

probability theory in a subjective perspective in uncertain and risky contexts.

This theory adopts several principles which form the basis of the classical vision: the principle of optimization - the decision maker endowed with perfect rationality given a set of alternatives will adopt the optimal choice with respect to the set objective; the principle of completeness - the individual has the ability to create expectations in terms of probability about the states and the consequences of his choices; the principle of transitivity - the decision is taken in an orderly and coherent way; the principle of dominance - the decision maker is able to attribute personal preferences to each alternative such as to allow him to prefer the best choice.

In order to be able to choose his own alternatives in a rational way, the rational subject "in the classical sense" has at his disposal all the possible information concerning the field of decisions and uses them in a fully efficient way. However, the following conditions must exist for the agent:

- decidability: always being able to decide which means to use for one's own ends,

- perfectibility: the individual has unlimited computational skills and perfect information on alternatives;

- asociality: no sociological influence can influence the individual's choices[2].

---

[2] Lanzi, D. (2007). Introduzione alla Teoria della Scelta Razionale. *Dip. di Scienze Economiche, Facoltà di Economia, Università degli Studi di Bologna.*

The decision problem in different areas of real life and in certain circumstances can be particularly complex.

There are two factors that characterize decisions: predetermined factors, which represent constraints; and variable factors. In the hypothesis in which a decision-making process registers an increase in predetermined factors, this certainly becomes more articulated assuming that the decision-maker could be faced with multiple and different alternative choices.

Furthermore, in order for an evaluation of all the alternatives to be carried out in a perfectly rational way, the decision maker should have a perfect knowledge and completeness of all the information that is useful for obtaining the optimal choice.

With the introduction of various information systems, it has been possible to witness a significant increase in the amount of information that can be found by decision-makers, as well as greater processing capacity making it easier to manage data sources and information processing processes.

These systems are part of the so-called Decision Support Systems: these are tools that help the decision maker through databases and the construction of mathematical models aimed at analyzing and solving complex problems.

In the following sections, the salient aspects of this discipline, which is as interesting as it is heterogeneous in its application, will be dealt with in detail.

1.2 Theoretical conceptualizations of the decision

Within decision theory there are different ways of analyzing a decision problem and of using appropriate models that influence the analysis of decision-making processes. In the literature, reference is essentially made to two main theories or decision-making paradigms that describe a different approach to the analysis and structuring of decision-making processes.

The rational decision-making process: the rational approach is configured in the normative type theory and aims, as its ultimate goal, the search for the optimal solution. The main characteristics of the rational choice process are identified in the decision maker's ability to identify all possible alternative solutions, for each of them to establish the relative consequences based on the cause-effect relationship, and to build a system of preferences or utility that they will allow him to perfectly order the options he has available. Therefore, the decision-making process structured by a rational decision-maker takes the form of identifying optimal choices, as a result of the maximization or minimization of a variable or function.

In particular, this approach is modeled by the maximization of expected utility. In this context, the concept of utility is understood as the degree of satisfaction that the individual derives from the immediate or future availability of a material or immaterial asset. Once the utility function[3] has been assigned to each alternative, the rational individual will choose the

[3] Morgenstern, O., & Von Neumann, J. (1953). *Theory of games and economic behavior*. Princeton university press.

one that maximizes his level of expected utility[4], defined as the average of the utilities of the individual outcomes, weighted by the respective probabilities:

$$U = \sum_{i=1}^{n} p_i u(w_i) \tag{1.1}$$

Were:

p_i - probability of occurrence of single outcomes,

u - utility of individual outcomes,

w_i - weight associated with the utility.

The rational decision-making process has highlighted some important limitations that prevent its application in real concrete contexts. The main limitations arise from the fact that the real decision maker does not have total and complete knowledge, is unable to define all the possible alternatives, and does not have the absolute ability to choose the optimal solution for the defined utility function.

---

[4] The utility function has been considered differently in the various currents of economic thought:

- for Fisher (1930) utility is synonymous with desirability: one of the elements that contribute to identifying the economic nature of an asset and arises from the relationship that is established between man and the good itself;
- for Marginalism, utility is considered as measurable in its cardinal sense: it allows mathematically to determine the quantity function of the good;
- for the Pareto theory utility is not a measurable quantity, but merely comparable.

These limits lay the foundations for the creation of mathematical models suitable for solving concrete problems, the decision maker often finds himself facing real problems that are characterized by a particularly high degree of complexity.

These issues have led several scientific studies to overcome the rationalist approach by introducing the concept of satisfactory decision making. By satisfactory choice we mean the decision obtained by reducing the computational complexity of a decision problem characterized by multiple interrelationships between the elements that compose it.

In the work "An Introduction to General Systems Thinking", Weinberg in 1975[5] suggests solving complex and uncertain decision-making problems through three aspects:

- The context of the decision-making problem must be thoroughly analyzed in order to reduce uncertainty by identifying all relevant elements;
- The states of the analyzed problem must be simplified by combining the elements that are not essential;
- The factors that are independent of each other, therefore that do not have interactions between them, must be combined to eliminate redundant elements as much as possible.

The main criticism of the model described by normative theory has struck the fundamental requirement, that is, the axiom of rationality; in fact, empirical observations demonstrate the difficulty of the decision maker in real contexts to assume perfectly rational behaviors. In the

[5]Weinberg, GM (2001). An introduction to general systems thinking (silver anniversary ed.). Dorset House Publishing Co., Inc ..

literature, in this regard, the concept of bounded rationality is proposed, introduced by the Nobel laureate Herbert Simon[6]in his most famous work *"Administrative behavior"*[7].This approach is based on two relevant aspects: cognitive limitations and the existence of a complex environment in which the decision maker finds himself acting. Especially in complex problems it is extremely difficult to make an optimal decision because the resources available relevant to analyze the information are limited, moreover the individual does not have the ability to fully understand the complex situations and interrelationships that exist between its components. .

The author has formalized some fundamental assumptions underlying the theory of bounded rationality: the impossibility of selecting all the options of a decision problem as well as the difficulty of assigning the relative probabilities; impossibility of modeling a utility function that contains all the useful criteria to perfectly express the preferences of decision makers (decision-making problems in the real context are multidimensional); information plays a fundamental role and the lack of availability conditions the search for a solution.

According to the limited rationality model, the strategies for solving a complex decision-making problem are based on heuristic processes, understood as rules of behavior that each individual implements for the resolution of a problem in order to reach the final goal. However, these heuristics can produce cognitive biases, that is systematic distortions of

---

[6]Economist and automation theorist Nobel Prize in Economics in 1978.

[7]Simon, HA (1950). Administrative behavior (p. 125). New York: Macmillan. This work has brought about a significant evolution in the study of microeconomics.

reasoning that lead the decision maker to pursue not the optimal decision but the satisfactory solution (satisficing criterion).

The decision-making process outlined by Simon has three main stages: intelligence, design and choice.

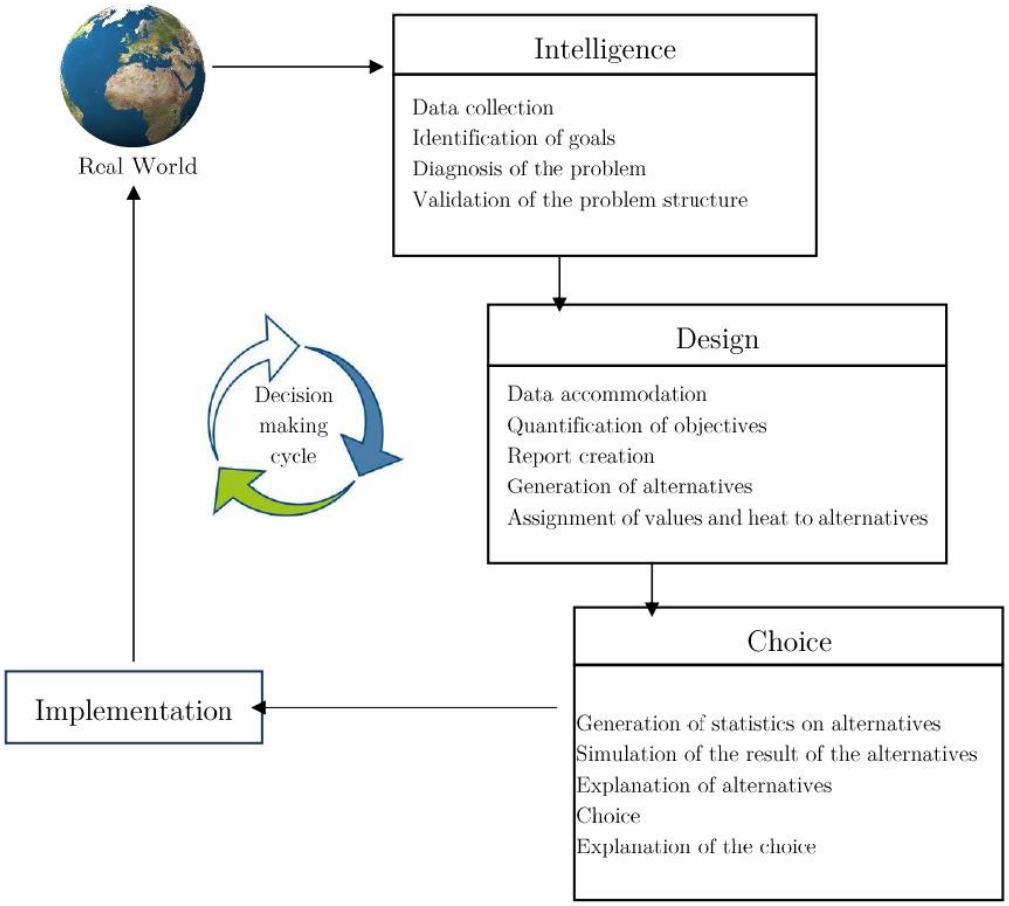


Figure 1: Main Stages of decision making process

In the intelligence phase, all those activities of collecting useful information from the surrounding context are carried out; the next phase of planning is concretized in the selection of the criteria to be used to compare the possible alternatives for solving the decision problem; up to the last phase of choice, in which the application of the selected criteria

(possibly weighted by mathematical models) allow to obtain the best solution.

The phases introduced by the model are interrelated by a feedback relationship such that each phase can affect the previous ones: if the decision maker is not satisfied with the result obtained in the individual phases, he implements a feedback mechanism to the previous phases by making changes to the individual activities deemed necessary to resume the process more effectively and efficiently.

This vision has led to an evolution of the decision-making process initially seen as a set of sequential phases to be carried out in order to obtain the final choice, in a cyclical procedure of phases where the complete execution of this decision-making procedure takes place through subsequent corrections.

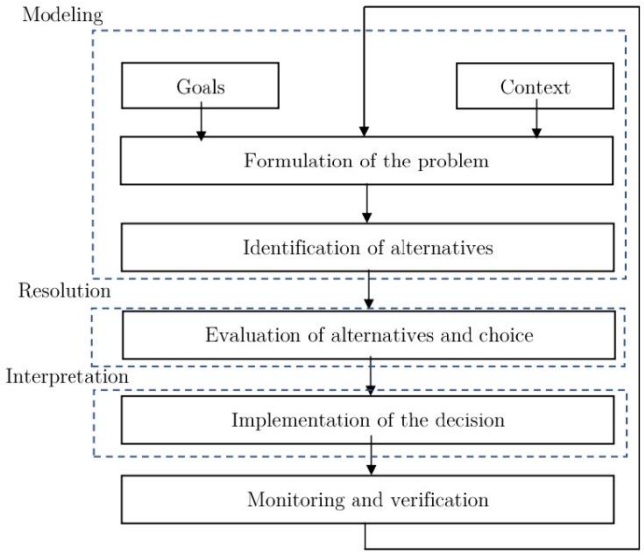


Figure 2: Decision process of rationality model

The Figure illustrates the procedure schematized by HA Simon in his fundamental work "Models of bounded rationality" (1982) 1- [HA Simon,

was one of the founders of Artificial Intelligence in the 1950s and won the Nobel Prize for Economics in 1978 for his studies on bounded rationality].

The scheme that represents the phases in which a decision-making process is divided:

- formulation of the problem: the system is circumscribed, identifying impacts and preferences on the one hand (Objectives), decision-makers and scenarios on the other (Context). In particular, the analysis of the reference environment, of the data and information available must allow him to promptly perceive the need for his intervention and to clearly define the decisions to be taken.
- identification of alternatives: the set of admissible alternatives is defined; that is, consistent with strategic priorities and assesses the consequences of potential action plans with respect to them.
- evaluation of alternatives and choice:

- the impact associated with each alternative and scenario is assessed;
- an alternative is chosen based on the preferences of decision makers;

- implementation of the decision:

the chosen alternative is translated into practice or simulated;

- monitoring and verification:

- the consequences of the decision are observed;
- if unsatisfactory, the process is adjusted and repeated by introducing new scenarios, new objectives, new alternatives, new evaluation methods.

According to Simon, in most cases the decision maker does not reach an optimal solution but is satisfied with a choice which corresponds to an acceptable performance value with respect to a fixed objective. This is why Simon's model is also known as the limited rationality model.

The model promoted by Simon has registered applications in various sectors including economics, psychology, management of organizations.

From the careful examination just explained it emerges that classical decision theory is no longer suitable for addressing choice problems in real contexts, where the search for solutions takes place in a highly laborious environment such as to determine an increase in the complexity of the decision problem.

It is therefore necessary to structure a different modeling useful for solving complex choice problems in real situations.

The most recent research investigates new theoretical frameworks in terms of decision making. The evolution of decision-making processes, the introduction of additional tools that support the choice activity as well as the innovation of information technologies, are the main events that led to the introduction of Decision Support Systems.

1.3 Decision support systems

As emerged from the analysis, in recent years we have witnessed an increase in the complexity of the systems, generating the need to introduce new methods for solving decision-making problems, the so-called decision support systems.

By decision support systems we mean the set of mathematical models and systems in general to support decisions relating to unstructured or semi-structured problems, which are difficult to find a solution with the use of traditional models.

In the scientific literature there is no single definition of these tools, but there are several definitions of a general nature proposed by different authors.

Kenn and Morton in 1978 they believe that decision support systems "combine the resources available to the individual with the abilities and resources of the computer to improve the quality of the decision". In 1994 Finlay defined DSS as "systems based on the use of computers to aid decision making". For Turban these are "interactive, flexible and adaptable information systems, developed in particular to support and improve the solution of unstructured management problems" (1995).

On a conceptual level it can be defined as: "computerized information system consisting of a set of procedures based on models to process data in close interaction with the decision maker, allowing an expansion of his problem solving skills."

From the definitional aspect, therefore, a common objective emerges: decision support systems allow the extraction and processing from a mass of data of the most useful information to support the decision-making process, in a more effective, flexible and rapid way.

With the introduction of these systems, the decision-making scheme proposed by Von Neumann undergoes a significant change. The three phases of the classic decision-making process; data acquisition - input phase -, data and information processing - processing phase - and presentation of results and processing - output phase -; they point out some weaknesses: in the first phase it is difficult to manage the large amount of data and information that should be processed effectively and efficiently; in the processing phase there is an obvious difficulty in calculating by an individual a large number of data, criteria within a limited time limit; in

the last phase it is difficult to always maintain congruence between the solutions of the decision-making problem with the pre-established objectives.

In this perspective, the introduction of systems to support the decision-making process makes it possible to help the decision-maker in each of the phases outlined. Through specific tools, the process of processing multiple data is made more effective and efficient by extrapolating only the information deemed relevant for the process; the different DSS models possess a remarkable computational capacity that allow to examine even very complex algorithms; thanks to these skills, these systems ensure greater consistency between results and objectives.

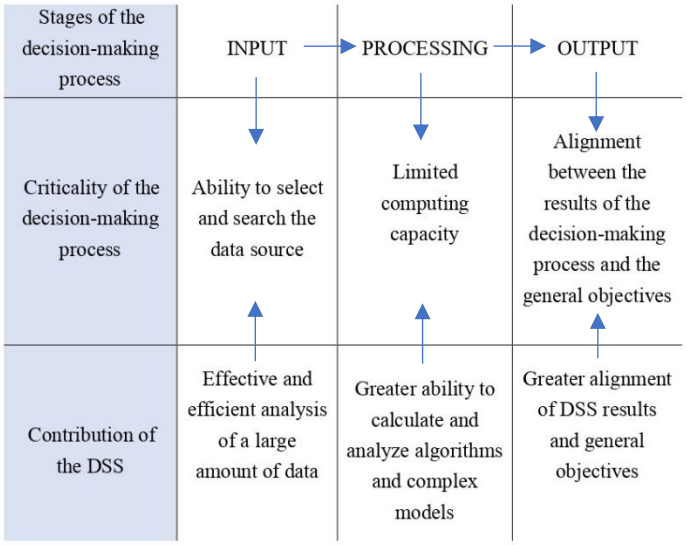


Figure 3: Stages of the decision-making process

Decision support systems are made up of several elements such as methodologies, models and information systems that follow a logical scheme of connection between the decision-making problem and the DDS model.

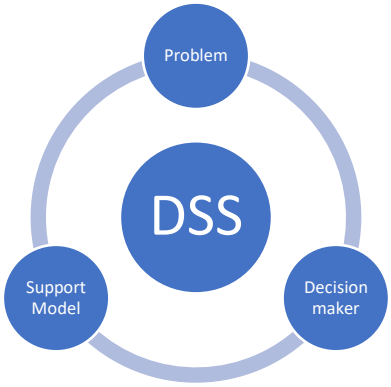


Figure 4: Main elements of Decision Support System

The fields of application of the aforementioned methodologies are many, they are useful in investment choices, in the design of technological systems, in production planning in the management of a project and concern sectors ranging from economics, engineering, architecture and so on.

The advantages of decision support systems are considerable, first of all they are tools that support the decision-maker in the management of complex semi-structured and unstructured problems, it should be emphasized that they do not replace the decision-maker, they also allow for greater efficiency and effectiveness of the decision-making process.

The expansion of different tools attached to the DSS was determined by the need to tackle several complex decision-making problems in which the main strategic resources are information and knowledge and which differ in specific characteristics.

1.4 The complexity of deciding

The modern era is characterized by ever more sudden and unexpected changes that affect different areas, from politics, to economics, to technology, making it extremely difficult to take the best decision since we find ourselves in an extremely complex context.

In today's world, the social and organizational reality is characterized by correlated and interdependent variables, actions and dynamics that produce effects both locally and globally; the ever more sudden and unexpected changes affect various fields, from politics, to the economy, to technology, making the decision-making process extremely difficult. A context influenced by elements of complexity emerges, where the tools and approaches used in the past are not adequate, highlighting the need to introduce new skills and strategies suitable for managing uncertainty and complexity.

Complexity originates from two aspects; firstly, reality has undergone such an evolution as to acquire the characteristic of complexity, we will soon see how globalization and the introduction of the Internet has made the world more interconnected; moreover, the analysis perspective has become more complex.

The increase in the complexity of the Western world is due to some fundamental stages of history such as the second industrial revolution, imperialism, and in the modern era the introduction of new means of transport and communication, and an economy that based more and more on close relationships. All this has characterized the new reality making it more and more interconnected. The progress recorded in the various fields has made the world more complex such as to determine a change in the

way of understanding, of knowing: in this case we are talking about the second scientific revolution (relativity, quantum physics, etc.).

Globalization, the Internet and technological development are key elements in the complexity of today's world understood as phenomena resulting from complex interactions. Being able to decipher such a complex reality is not a simple task; therefore, it is necessary to adopt the so-called reticular thinking which is more suitable for interpreting the events of the new planetary dimension.

From this point of view, the thought of complexity was born, aimed at wider and interdisciplinary areas, which consists of a new approach to tackle problems by considering more sectors of knowledge.

Central role within the theory of complexity is played by the concept of system. Complex systems have two important characteristics: the network structure, which consists of a continuous interaction between the different components of the system; and feedback, understood as feedback, that is, every consequence has an effect on the cause. Since systems are characterized by the set of relationships (the network), a method in which the individual parts that compose it are studied is not suitable, but the complex must be examined to understand each elementary component.

Complex systems are composed of a plurality of components that interact with each other through a reticular structure. The globalized world represents the main complex system characterized by close connections - in different sectors such as political, economic, social, cultural - between the different elements - countries, companies, institutions. This implies that the variations that occur in the single element can determine consequences for the global system and vice versa.

The complexity of these systems is determined by the following relevant characteristics: the presence of a large number of components connected to each other by lattice relationships, complex representation in analytical terms of the elements of the system, difficulty in evaluating the parameters, intense interaction with other systems and with the external context.

The complexity of the systems can be interpreted as a forecasting difficulty, understood as a difficulty in representing in detail the future evolution of a given system; control difficulties, ie it is complicated to impose a predefined direction on the system; calculation difficulties, find the best solution to specific problems quickly; modeling difficulties, in terms of understanding and structuring the system at a qualitative and quantitative level due to the influences of exogenous factors.

In 1962 the Nobel Prize in Economics Herbert Simon provides the following definition of complexity in the article The Architecture of Complexity[8]:

> *"I shall not undertake a formal definition of complex systems. Roughly, by a complex system I mean one made up of a large number of parts that interact in a nonsimple way. In such systems the whole is more than the sum of the parts, not in an ultimate, metaphysical sense but in the important pragmatic sense that, given the properties of the parts and the laws of their interaction, it is not a trivial matter to infer the properties of the whole. (Simon, Gell-Mann and Lloyd on complex systems) In the face of complexity an*

[8] Simon, H. A. (1962). The Architecture of Complexity. *Proceedings of the American Philosophical Society*, *106*(6), 467–482. http://www.jstor.org/stable/985254

in-principle reductionist may be at the same time a pragmatic holist".

From this definition a fundamental aspect of complexity emerges, that is the hierarchical nature as a complex system is structured by sub-elements which in turn are composed of further sub-elements and so on, in this way the complex structures organized in a hierarchical form can be broken down into elementary sections to study them more quickly and dynamically.

Another element of difficulty is represented by the impossibility of attributing precise qualities and giving an absolute measure to complexity.

In this perspective, in order to better manage the growing complexity, an interdisciplinary approach based on a progressive elaboration is necessary, where the ability to interpret the evolution of the context; therefore, seeing in advance the effects of different actions, assessing future risks and opportunities, becomes a decisive element in making the best decisions.

The future of Jobs report published by the World Economic Forum in 2016 predicted, in terms of the dynamics of the labor market, an evolution of fundamental skills, in particular the main reference is to the ability of complex problem solving[9].

[9] World Economic Forum. (2020). The future of jobs report 2020. Retrieved from Geneva

The various sectors of reference, such as industrial production, finance and the mobility sector, in the period from 2015 to 2020, recorded about 40% of the obsolescence rate of traditional skills with a growing attention to new skills: decision-making capacity in conditions of complexity, critical thinking, judgment skills in decision-making processes.

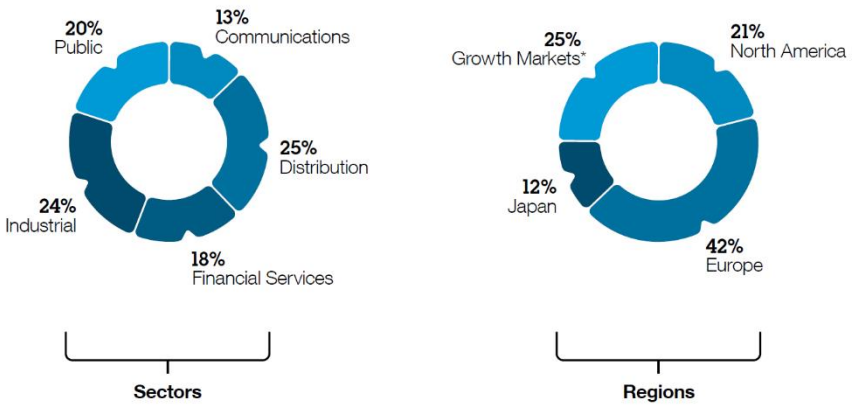


Figure 5: Sectors and Regions of participated in this study

In the literature, various documents pay particular attention to the issue of complexity, including the work carried out by IBM Corporation in 2009[10]. This study involved about 1500 CEOs of the largest companies and public organizations around the world, underlining that "exponential growth and rapid complexity represented the most important challenge perceived by CEOs for the next few years".

It emerged from the interviews that the context in which we operate is characterized by ever increasing volatility, uncertainty and complexity. In fact, there may be sudden fluctuations in the economic, product and innovation cycles from which greater associated risks arise; uncertainty is

[10] IBM Institute for Business Value (2009), Capitalizing on Complexity Insights from the Global Chief Executive Officer Study.

linked to the difficulty of predicting changes in the various competitive, technological, social, regulatory, geopolitical, environmental contexts; moreover, the interconnections and interdependencies between volatility and uncertainty lead to greater complexity.

Furthermore, in terms of interconnections and interdependencies, the digital revolution and the processes of globalization have amplified these aspects worldwide, recording a result of over 3 billion people reached by information and telecommunication technologies. Nowadays we are invaded by enormous amounts of information and we constantly relate to others by generating close connections such as to determine an immediate transmission of events in every part of the world. Interconnections are now structured at any level by financial markets, energy and transport networks, businesses and ecosystems in which they operate, citizens, countries and this influences individual and collective behaviors and decisions of the entire planet.

Therefore, complexity in this context is understood as an increase in interconnections and interdependencies such as to make it difficult to predict the occurrence of specific phenomena. It is worth mentioning in particular the consequences of two historical phenomena characterized by complexity: the crisis of 2008, in which the strong interconnection of financial markets had negative effects on the world economy; the Coronavirus pandemic in 2020, where the interconnection between different countries has produced dramatic consequences at an international level.

It is clear that in the face of a complex system, adopting traditional measures determines the failure of the actions to resolve these phenomena; therefore, it is necessary to increase new skills and new paradigms of action

suitable for better managing the complexity generated by interdependencies and interconnections.

According to Edgard Morin, philosopher of complexity "the positive aspect, the progressive aspect that can derive from the response to the challenge of complexity consists in taking off towards a multidimensional thought."

Another element that has contributed to taking the concept of complexity to the extreme is the external factor of technology which has recorded a significant increase in the interconnections of various systems globally. We live in a hyper-connected world and therefore the outcomes of any decision can have consequences in multiple systems and at a high speed, beyond the boundaries of a discipline, a process, an industry, a nation.

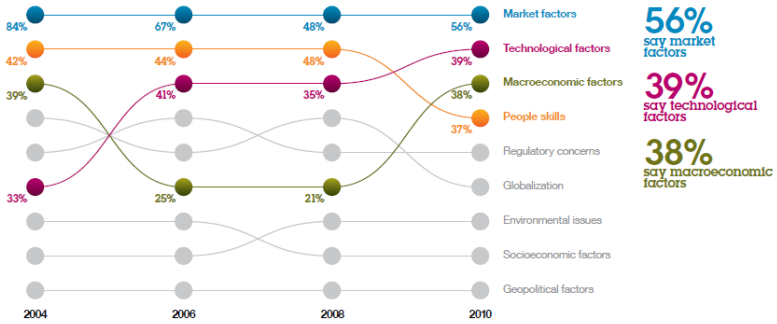


Figure 6: Top external factors. The relative impact of technology as an external factor rises year on year.

The CEOs expressed their concern about the new economic context in which they operate, finding greater volatility, a more uncertain environment, with increasing elements of complexity and structurally in continuous evolution; *"A true paradigm shift that is revolutionizing not only business, but also global social structures".*

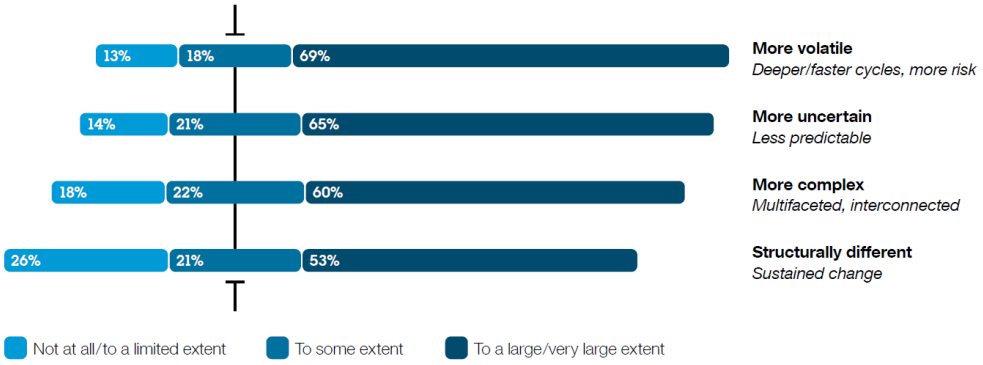


Figure 7: Organizations are experiencing significant upheaval

In this regard, an interesting analysis relating to these aspects is mentioned in the Global Risk Report of the World Economic Forum (The Global Risks Report 2022, 17th Edition, is published by the World Economic Forum). This work analyzes the main risk factors such as extreme climate events, the failure of climate change mitigation policies, cyber and data security, large-scale immigration, financial bubbles in some key sectors, fragmented terrorism; factors that characterize society and the current economy. The consequence of the interconnection of each risk factor with the others concerns the possibility of causing a domino effect such as to characterize decisions on individual risk factors.

There are guidelines in the literature for dealing with complexity. It is considered appropriate to adopt strategies aimed at decomposing and standardizing complex problems; the sub-systems thus obtained must be analyzed one by one in order to determine the most relevant elements. These phases are characterized by continuous processes of coordination and conjunction.

In the management of complex systems it is difficult to arrive at the global optimal solution, which is why the process of bounded rationality is

adopted which allows to obtain compromise solutions between all the most significant variables and parameters (local optimal or heuristic solution).

1.5 Decision is knowledge

The ability to make the best decision is characterized by a careful analysis of all possible results through a perfect scientific knowledge of the problem.

According to the classical paradigm, conditioned by the philosopher and mathematician Descartes, certain knowledge is based on two axioms: The first is based on the concept of dividing the problem under consideration into several parts, first looking for solutions for the simpler elements, and subsequently bringing back the single results to the final solution of the problem by recomposition. The second axiom is based on the concept of neutrality of the observer, as a fundamental element for knowledge to be certain and objective.

The classical vision is characterized by three aspects concerning the search for certain, objective and universal knowledge.

The first aspect is determinism, according to which every phenomenon is caused by a previous event on the basis of a mechanistic cause-effect relationship. In the context under examination, scientific knowledge is associated with the ability to predict future effects starting from the determination of causes (principle of causality). Knowledge is therefore understood as a predictive science, which through the study of causes identifies the universal laws obtaining the prediction of the effects and therefore of the future.

This conception has been superseded by modern approaches such as data processing and analysis as well as the introduction of artificial intelligence as more suitable tools in the context of complex systems. Despite this, deterministic approaches can also occur in modern times: the director of MIT Connections Science, Alex Pentland, believes that “big data gives us the opportunity to see all the complexity of society through millions of networks of exchanges between individuals. . If we could endow ourselves with the almighty gaze of God, we could theoretically arrive at a real understanding of society and work hard to be able to solve its problems “; thus bringing out the deterministic aspect of the concept of predictive knowledge.

Reductionism, on the other hand, is the approach according to which the whole is equivalent to the sum of its parts. Therefore, the knowledge of a complex phenomenon takes place through its decomposition into elementary partitions, by subsequently recomposing the partial solutions, one reaches the total knowledge of the phenomenon.

Knowledge is also conditioned by rationalism, that is, by the philosophical aspect according to which reason is at the center of knowledge of every aspect of reality, the only element that highlights the ability of subjects to acquire true knowledge, while all the other aspects represent disturbing elements. This concept is criticized by the neuroscientist Antonio Damasio who demonstrates that in terms of the quality of the reasoning “An excess of feeling in the narrower configuration or a lack of feeling in the larger one can have disastrous consequences.” 1 “It is as if we were possessed from a passion for reason:

The classical approach to knowledge based on these three pillars registers a progressive decline starting from the new conception of a not

perfectly ordered world with respect to which it becomes more difficult to acquire a perfect knowledge of all phenomena. In particular, the idea of a world comparable to a machine that works indefinitely is lost due to the science of thermodynamics which demonstrates the degradation of energy due to the increase in entropy. Furthermore, Max Planck discovers the quantum of energy, making the particles of matter not perfectly definable, identifiable and measurable; characterized by the subjectivity of the observer, putting in crisis the neutrality of the same, one of the key elements at the base of the classical approach.

According to the illustrious physicist, even the notion of absolute truth is emptied: "To the extent that the propositions of mathematics refer to reality, they are not certain comma and to the extent that they are certain they do not refer to reality"[11].

Further criticism was introduced by the uncertainty principle[12]by Warner Heisenberg who states that:

> *"It is not possible to determine with arbitrary precision and simultaneously two conjugate variables, that is, it is not possible to know exactly and simultaneously two variables such as position and momentum of a particle".*

---

[11] De Gandt, F. (2006, June). Geometry and experience: Einstein's 1921 paper and Hilbert's axiomatic system. In *AIP Conference Proceedings* (Vol. 841, No. 1, pp. 285-290). American Institute of Physics.

This famous phrase has often been mentioned by students of the Fuzzy theory.

[12]Heisenberg almost never used the noun principle. His most used terms were Ungenauikeitsrelationen (inaccuracy relations), Unsicherheitrelationen (uncertainty relations) and Unbestimmtheitsrelazionen (uncertainty relations) [D. Lindley, 2008]. It was only in 2013, 86 years after Heisenberg's original article of 1927, that a way was found to derive its uncertainty relations from the postulates of quantum mechanics.

The strong formulation of the principle of causality is questioned according to which “perfect knowledge of the present allows us to predict the future”, since it is not possible to know in detail the present in every element of determination and consequently to predict with certainty the effects future.

The modern approach therefore attributes to the concept of knowledge elements of chance, disorder and uncertainty that do not allow the prediction of the future aspects of complex systems.

At the end of this examination it is possible to understand that the classical approach gives way to the sciences of probability and statistics.

In conclusion, it is necessary to understand that the context in which we act is not linear, it is not perfectly predictable, it is intrinsic to paradoxes and conflicting choices; reality is interconnected and interdependent; therefore, all the decisions taken generate effects such as to be potential elements of reconfiguration of the system in which we operate. It becomes essential to understand the complexity of the context in order to avoid or at least limit the consequences of the choices that can occur not only locally but also globally.

On the basis of these considerations it can be understood that complexity cannot and must not be eliminated but must be mastered, or even complexity must be brought to one's advantage; this is possible through an iterative approach to strategy and the ability to develop faster and more effective decision-making processes.

This can be achieved through the introduction of new models, methods and tools that make it possible to concretely support the taking of decisions in complex contexts, among which a careful examination of Multicriterial Methods will follow.

In this regard, there has been an important evolution from a technological point of view, in particular, great expectations are placed on the so-called big data and artificial intelligence.

1.6 The Complexity of "Deciding" at the time of Covid-19: Some Thematic Reflections.

All decision-makers at all levels must make adequate decisions in a context of rapid change: just think that the information on the pandemic, the data on infections, deaths and healed follow one another continuously. Furthermore, the decision-making process is made even more complex by a fundamental constant: uncertainty.

Institutions have been called upon to take fundamental decisions: "close everything, block countries from a suspended life". There is a need to find solutions that take into account the global crisis in which, perhaps inevitably, we found ourselves. The choices are complex and difficult because a trade-off must be considered: remain closed to protect health or reopen everything to support the economy? This is the main compromise but it is not the only one to which the rulers are called to make certain choices: "How to close? Which supply chain to leave open? How to reopen? Which supply chains to reopen first? What can be allowed and what not?"

In this period we have experienced the complexity of deciding taken to the extreme of the dramatic situation of Covid-19, consequently it was found that the structuring of decision-making processes has undergone changes due to the coronavirus and problems socio-economic ensuing: there are very strong signs which reveal how following the old course of action is incompatible with the new objectives and the different priorities. It is

necessary to take into account the plurality of interests that must be taken into consideration: health, work, economic development but also privacy (with reference to the application that allows the tracing of the infection).

Among the decisional aspects to be examined there is uncertainty: The uncertainty relates to the very limited knowledge, which is being acquired with great difficulty about the nature of the virus, also linked to the reaction of the economic system to such extreme conditions.

In this perspective, some reflections related to the issue of the decision can give interesting interpretations of the current situation.

There was a large use of experts to whom it was decided to resort, there are at least fifteen task forces appointed by the government. These experts are reproached for not having a single and clear position: the position of science.

In this regard, it is good to reflect on the sense of ignorance: we ignore the exact number of infected people, even there has been and continues to be a discussion about what it must mean to die of coronavirus and how the deaths from COVID-19 should be counted. But attention is primarily focused on the evolution of the contagion and therefore on the models that describe it and make it possible to make predictions.

As a first approximation, no model will be able to tell us exactly what the number of hospitalized for coronavirus will be tomorrow, in three weeks, in a month; we could only estimate a probability distribution. We can define the Calculus of Probabilities as the mathematical theory of uncertainty. Like any mathematical model, even the probabilistic one, on the one hand, allows the treatment of a problem of interest in a logical and rigorous way; on the other, it necessarily represents an abstraction of reality and captures only some aspects of it. The model must lead to “useful”

results, which are in agreement with the experimental evidence, this depends on the basic assumptions and hypotheses; therefore the probability-based model does not have an objective consistency.

It is precisely possible to distinguish four types of probabilities: classical probability, frequentist probabilistic model, subjective probability, axiomatic probabilistic model.

Classical probability. The probability of an event is the quotient between the number of favorable cases and the number of possible cases, when they are all equally possible:

$$p(E) = \frac{f}{u}$$

Where is it:

p = probability

E = event

f = number of favorable cases

u = number of possible cases.

If an event is impossible, the number of favorable cases is 0, so:

$$p = \frac{f}{u} = \frac{0}{u} = 0$$

Therefore the probability of an impossible event is 0.

If an event is certain, the number of favorable cases is equal to that of possible cases, so:

$$p = \frac{f}{u} = \frac{u}{u} = 1$$

The probability of a certain event is 1.

For random events, the number of favorable cases is between 0 and u:

$$0 < f < u$$

By dividing all terms of the double inequality by u, we obtain:

$$\frac{0}{u} < \frac{f}{u} < \frac{u}{u}; \quad ossia \qquad 0 < p < 1$$

Therefore the probability of a random event is a number between 0 and 1. The sum of the probabilities of an event (E) and that of its opposite event ($\bar{E}$) is 1:

$$p(E) + p(\bar{E}) = 1$$

Frequentist probabilistic model. Probability is the limit of the proportion of times event A occurs in a very large number n of repetitions of a random experiment

$$P(A) = \lim_{n \to \infty} \frac{n(A)}{n}$$

Where is it:

$n(A) =$ is the number of successes in the first n experiments

$\frac{n(A)}{n} =$ is the relative frequency of event A.

Subjective probability. Probability expresses the individual's level of confidence in the occurrence of a certain event. Therefore, decision-makers with different information can evaluate the occurrence of an event with different probabilities.

The probability of an event must be seen as the degree of confidence that each one attributes on the basis of the state of information upon the occurrence of the event.

To evaluate the subjective probability of the event just propose a bet: it will win a certain sum if the event occurs otherwise nothing.

The price $P(A)$ that is considered fair to pay for this bet is given by:

$$P(A) = \frac{p_A}{S}$$

The problem of this model is that the price may not reflect the truth. The solution is that the decision-maker declares the fair price before he knows he is the bettor or the dealer.

The principle of consistency states that whoever evaluates the probability will never do so in order to be forced to accept a betting system in which it is definitely placed at a loss.

Axiomatic probabilistic model. Kolmogorov's axiomatic approach can be seen as a codification of computational rules which are independent of the precise meaning attributed to probability.

The mathematical formulation of the probabilistic model consists of the whole Ω, B, P called probability space, and allows to assign a non-negative real number $P(Aj)$ which we call probability of Aj, to the events that form a Borel field B consisting of subsets of a sample space associated with the random experiment.

Let is Ω a finite sample space and A its event, the probability of event A consists of a real number following three axioms:

Axiom 1. $P(A) \geq 0$;

Axiom 2: $P(\Omega) = 1\ (normalization)$;

Axiom 3: $P(A \cup B) = P(A) + P(B)\ if\ A \cap B \neq \emptyset$

It can be found that each model gives its estimate of the probability, and as far as possible one comes to the conclusion that one must evaluate them all. These considerations are valid for most decisions, but these take on fundamental relevance for decisions relating to a completely new phenomenon, for which we not only do not know the future but do not even know the present.

Therefore it is important to underline the importance that we must not take into account a single model, but several models, even if different. In this regard, it is possible to mention the intervention of the economist Lars Peter Hansen - Nobel laureate for economics in 2013 - who, regarding the current situation, quotes a sentence from St. Thomas Aquinas: “I distrust the man of a book only”, converting this assertion to the topic dealt with: “distrust men (governments) who base their decisions on a single model”.

In such a context, it is impossible not to refer to two areas of interest:

- The Theory of Public Choice, developed by the American economist James Buchanan - Nobel laureate in economics in 1986 - adopts tools and methods of economic sciences by studying the behavior of makers in the political scene. Inevitably, decisions made regarding the Covid-19 pandemic fall within the scope of Public Choice (Gordon, Buchanan & Tullock 1962)

- The Analysis of Multicriteria decisions, an analysis that is part of the theory of decision support methods in which a plurality of points of view must be considered, in the case in question, it is considered necessary to find a compromise between public health, economy and privacy.

In these two fields of research one can find a rigorous but also realistic scientific approach to the issue of decisions. There are also references to a less theoretical and more technical approach based on the decision-making process that is Operations Research, a discipline that deals with the development and application of scientific methods for solving decision problems, using mathematical models. This approach provides useful tools to guide the expert in making a decision, the result of a convention built in the course of a process that requires multiple interactions, involving a variety of actors involved in a complex decision-making environment.

On the basis of these careful observations, it may be asked whether a combination of models can be considered particularly suitable for analyzing this specific problem. The solution lies not so much in combining existing methods or finding new ones, but in being able to understand what to put in place. In other words, you should define the problem and the questions you want to answer and then try to see how to answer those questions in a convincing way.

To support a decision-maker in deciding policies that take into consideration the health aspect and the economic aspect, it is necessary to try to put together on the one hand a SIR model that represents the spread of the pandemic as the containment measures vary and on the other a macroeconomic model that describes how those same measures reduce GDP or employment. Subsequently, a procedure should be found that makes it possible to represent in a simple and accessible way the results in terms of infected, hospitalized and deaths on the one hand and of decrease in GDP, unemployment and other variables of an economic nature on the other. There is a need for an additional tool that allows us to represent the preferences of the decision maker in the face of these quantities at stake. In the end, it would be good if all this were represented in a probabilistic and dynamic context. Therefore it is necessary to use various tools: epidemiological models, macroeconomic models, probabilistic models, decision support models. All this must be guided by the goal you want to achieve: helping the decision maker to better understand the decision problem and to form his own conviction in order to make a good decision consciously.

A further aspect that emerges in this situation is the psychological-behavioral approach which is now relevant in the economic field, in this

case we speak of Behavioral Economics. The behavioral approach affects the economic aspect since the individual's way of reacting depends on how the problem is exposed.

In this context, the Framing effect is considered which concerns the choice process in which a phase of disposition of the decision problem and an evaluation phase are distinguished. The latter is considered as a consequence of the former which assumes a central role in the model. In fact, the preference for one of the alternatives of a decision problem depends on how the problem itself is interpreted and presented, with the consequence that the result may be different by presenting the alternatives in a different way. The authors who brought to light these deviations from the rational choice model are Daniel Kahneman and Amos Tversky, through the Asian disease problem experiment (1981).

University of British Columbia students were asked to choose between two health plans due to an unusual Asian epidemic that predicts the loss of 600 people. Two intervention programs are proposed. The first program is presented in terms of lives saved, the choice is between: 200 people saved or 2/3 probability that no one is saved. The second in terms of lives lost: 400 people will die or 1/3 probability that no one will die.

It was found that, although the objective probability of outcomes is the same, if the questions are asked in terms of lives saved, individuals choose the least risky option; if, on the other hand, the questions are asked in terms of the number of deaths, the subjects choose the riskiest option.

They first subjected the experiment to students and, by reproposing the experiment to professional clinicians, showed that they too were prone to make the framing mistake (Kahneman & Tversky 1981).

Final considerations. I would like to conclude with an interesting clarification on the main theme of the entire reflection: "what is meant by the right decision? One could imagine that a good decision is the one that determines, as consequences, good results and therefore its goodness would be linked to its ex-post success. To explain this aspect, a quotation from Herodotus taken up by the economist Keynes is proposed: "Careful discernment is the greatest advantage: in fact, if one has chosen a good thing, even if some adversity occurs, the decision remains good, and it is at best only defeat by fate. On the other hand, whoever chooses lightly, even if fate accompanies him and makes a profit, has nevertheless been ill advised" (from Herodotus, Histories, book VII, 10).

Therefore a decision is not good ex-post because its results are good, but we can consider an ex-ante decision good if the process that led to that choice was good".

2 Chapter: Artificial Intelligence

2.1 Introductory concepts of Artificial Intelligence; 2.2 Development of Artificial Intelligence in the world; 2.3 Theoretical framework and history of AI; 2.4 Different approaches of Artificial Intelligence; 2.5 Algorithms and learning models.

2.1 Introductory concepts of Artificial Intelligence

The concept of Artificial Intelligence (AI) is often linked in collective thinking to aspects of futures connected to the creation of machines capable of acting perfectly like human beings, but this is not exactly the case for two reasons, first of all artificial intelligence does not refers only to the construction of so-called machines. humanoid robots and also because the expression does not refer to future aspects but artificial intelligence is already the present.

Identifying a precise definition of artificial intelligence is not easy since in the literature there is no single definition of AI this is also due to the rapid evolution that configures this treatment in different disciplinary fields. In the international scientific sector, AI on a conceptual level is recognized as a “discipline belonging to computer science that studies the theoretical foundations, methodologies and techniques that allow the

design of hardware systems and software program systems capable of providing the computer electronic performance that, a common observer, would seem to be of exclusive relevance to human intelligence "[13]

It is a science that welcomes the influences of multiple disciplines ranging from computer science, mathematics, economics, philosophy, neuroscience, psychology, cybernetics, cognitive sciences and linguistics. The potential of this discipline has provided an important contribution to the progress not only of some sectors but has determined a significant development of the entire society today.

Over time, the domain of artificial intelligence has assumed increasing importance on the part of researchers, scientists, companies, universities, this growing interest is due to the surprising ability of analysis and organization of a huge number of unstructured data, impossible to manage through the calculation skills of individuals.

For this reason, companies implement artificial intelligence in their organization to make more accurate decisions by exploiting the ability to analyze large amounts of data allowing the achievement of a better result and consequently the achievement of a significant competitive advantage.

In today's world, the primary resource for any organization at any level is information. It is essential to have the ability to archive, organize, and process information because from these it is possible to deduce insights at a forecasting level such as to make the organization more competitive in the adoption of specific strategies. the information is the result of an elaboration of the available data which in the current context are in

[13]Somalvico, M. (1987). Artificial intelligence. Science & new life.

enormous and ever increasing quantities, in fact, we are talking about the so-called big data. The man with the abilities of him is not able to carry out a precise and detailed evaluation of such data so as to be indispensable a suitable tool to work with the large amount of data, the

The concept of big data can be identified by its main characteristics: volume, speed, variety, variability, value, virality and truthfulness. With respect to the volume it was previously said that the main feature concerns the huge amount of data coming from different sources. The introduction of different channels from which to retrieve data has not only resulted in an increase in volume but has also affected the increase in the speed with which data is generated. this speed must be carefully considered by organizations to adapt their strategies quickly. moreover, the data available especially following the technological revolution derive from sources of a different nature so as to be considered unstructured and inhomogeneous, for this reason we speak of the variety of the data. compared to the large amount of data available, not all data are relevant or have the same importance, in this case we speak of variability; it is necessary to identify only those significant data that represent value for the organization. Virality means the ability to disseminate data, the possibility of sharing via the network allows continuous processing and constant updating of data, while the concept of truthfulness detects the degree of reliability of the data.

Nowadays it is possible to observe that the science of artificial intelligence is expanding on different application areas, from economic, financial, health, engineering, architectural and so on.

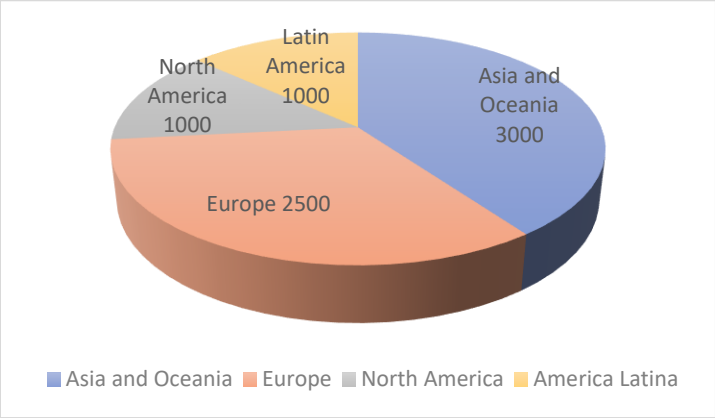
It was found that thanks to the implementation of artificial intelligence in all sectors, it will be possible to record considerable economic growth,

and in particular the factors that will determine a greater impact on this growth, according to the investment bank JP Morgan concern: resources human beings, the contribution of artificial intelligence in making workers more productive determines a growth in labor productivity; advantageous modification of the output, due to a greater attitude to personalize products and services; in terms of costs, the growing ability to generate more and more tools equipped with "intelligent technology" allows a reduction in costs; the security, an element that brings great interest in the current context thanks to the introduction of new techniques and new tools, it is possible to prevent and identify any cyber-attacks.

2.2 Development of Artificial Intelligence in the world

Through a survey conducted by the IBM Global AI Adoption Index[14] it is possible to analyze the growth of AI implementation in the world.

The survey carried out online in the period from 30 March to 12 April 2022 took as a research sample the main companies from all over the world, in particular a total of 7,500 companies were involved in Italy, Spain, France, Germany, United Kingdom, Canada, United States, Australia, China, South Korea, Singapore, India and United Arab Emirates (with 500 companies for each country), and Latin America (with 1000 companies in Brazil, Mexico, Colombia, Argentina, Chile and Peru).



Graphic 1: Search sample by geographical criterion. Source: IBM Global AI Adoption Index.

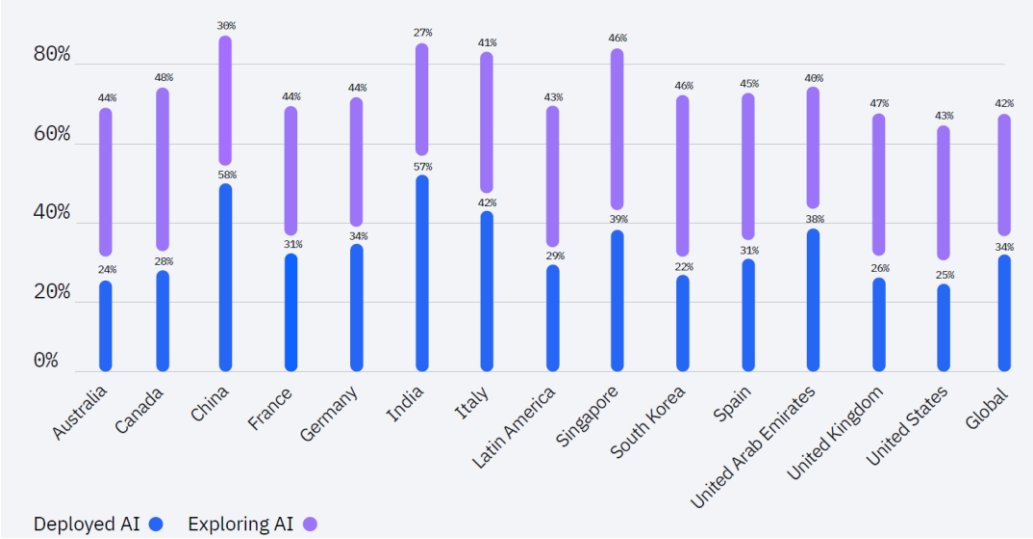
The work carried out recorded a share equal to 35% of the activities that adopted artificial intelligence technologies in 2022. Compared to 2021, the

[14] IBM Global AI Adoption Index (2022). New research commissioned by IBM in partnership with Morning Consult.

data just indicated highlights an increase of about 13% of organizations that have adopted artificial intelligence in the current year.

The survey carried out by IBM shows that the countries that occupy the top position in terms of the diffusion of artificial intelligence are China and India with a rate of about 60% of the market and with interesting growth prospects. This is also due to the continued support of research in this sector, with an exploration rate of 30% for China and 27% for India.

Singapore and the United Arab Emirates are also above the international average with adiffusion rate close to 40% and research rate in the sector at 46% and 40% respectively.

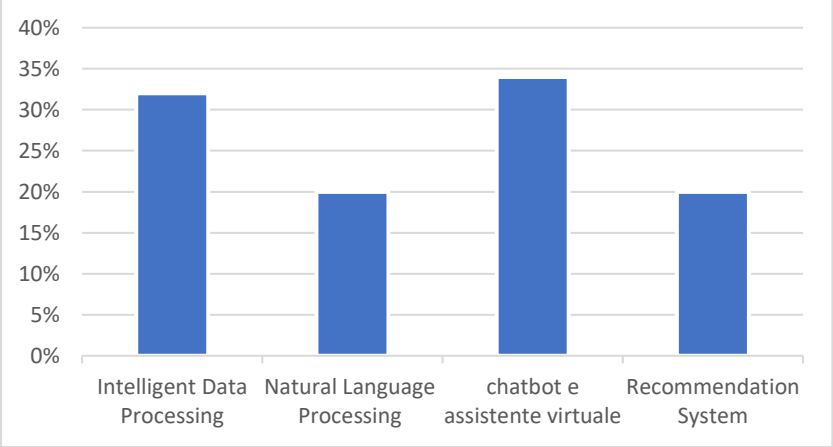


Graphic 2: AI adoption rates around the world. Source: IBM Global AI Adoption Index

Even the European market has recorded interesting results, it can in fact be noted that the West invests resources in research and enjoys the diffusion of AI technologies superior to America to Australia. Indeed, Italy is in third place in circulation with a percentage just over 40%. From the comparison with other European countries, the detailed analysis reveals a lower performance in terms of research in the field of artificial intelligence,

this data is also recorded compared to other countries at an international level.

Based on the data reported by the National Information Agency ANSA, the Italian artificial intelligence market records an investment of € 380 million[15](marked share + 27% in 2021). The main application areas to which these sums are destined are the insurance-financial, energy and industrial fields, the most exploited algorithms are chat bots and virtual assistants, Intelligent Data Processing algorithms, Natural Language Processing and recommendation system algorithms.



Graphic 3: Main types of AI. Source: IBM Global AI Adoption Index.

The survey was aimed at various small and large companies divided as follows: small companies with 50 employees for 21%, medium-sized companies with 51-250 employees for 20%; medium-large companies with

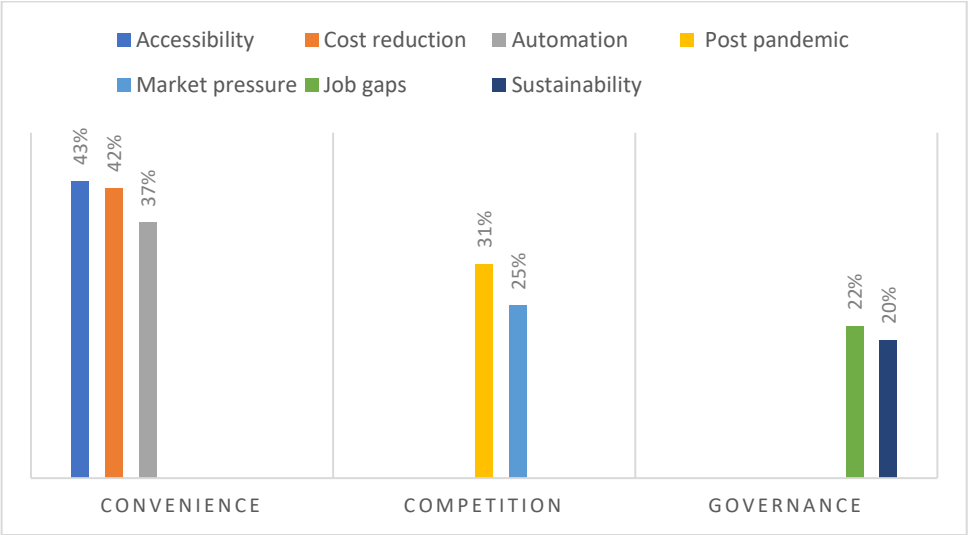
[15]Investments in the context of AI equal to 380 million euros are divided as follows: 76% from Italian companies, 24% commissioned from project exports.

251-1000 employees for 27% and large companies with more than 1000 employees for 32%.

In particular, in Italy there is a considerable gap between Italian small and medium-sized enterprises and large companies that have implemented "intelligent technology": the former amount to just 6%, while large companies reach 87%. This data highlights the need for interventions in support of small and medium-sized enterprises to promote a significant increase in this science in Italy.

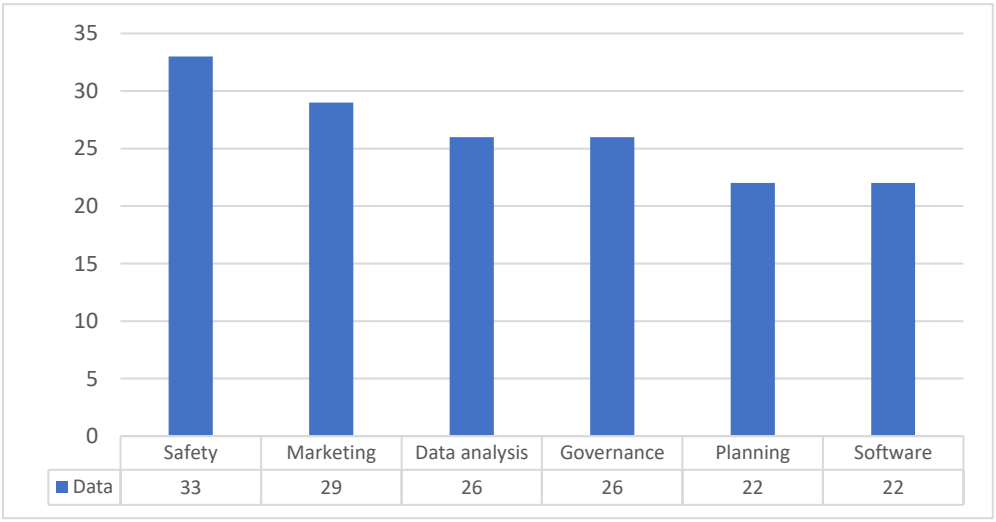
Another interesting fact that emerges from the survey carried out is that many companies create their own strategy by investing in artificial intelligence, believing that this can determine an advantage in the long term. There are three main elements that have influenced the use of AI technologies in companies: convenience, in terms of increasing the ability to access data and information; competition with competitors, understood as the ability to react to even unexpected and sudden changes[16], and corporate governance, in terms of sustainability and job gaps filled by artificial intelligence technology.

[16]Consider the unexpected and accelerated process of change recorded in recent years due to the Covid-19 pandemic.



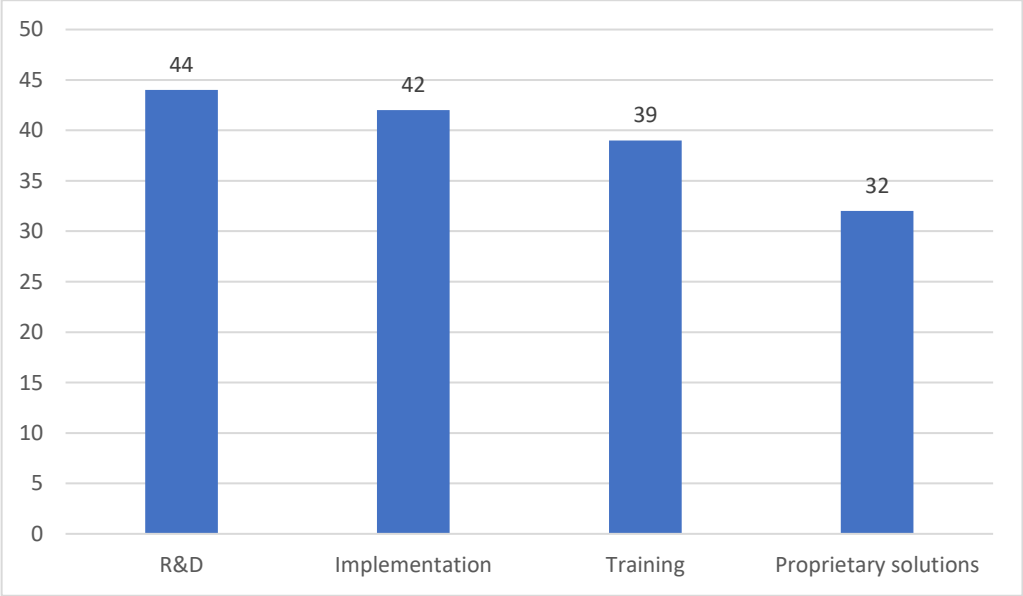
Graphic 4: Factors that determine the adoption of Artificial Intelligence in companies. Source: IBM Global AI Adoption Index.

With reference to the application areas of AI, the first place is reserved for the automation of company activities; in second place is information security, a sector that has reached this position in the recent context due to the growing interest in the protection of information; data analysis, financial planning and software production follow.



Graphic 5: Fields of application of Artificial Intelligence in companies. Source: IBM Global AI Adoption Index.

The IBM survey also highlighted the AI investment sectors that will be most affected in the future: it is estimated that 44% of companies will allocate part of their resources to research and development, 42% to technology in their company, 39% of companies believe that the best strategy is the training of highly qualified human resources, the remaining companies will invest in the development of proprietary solutions.

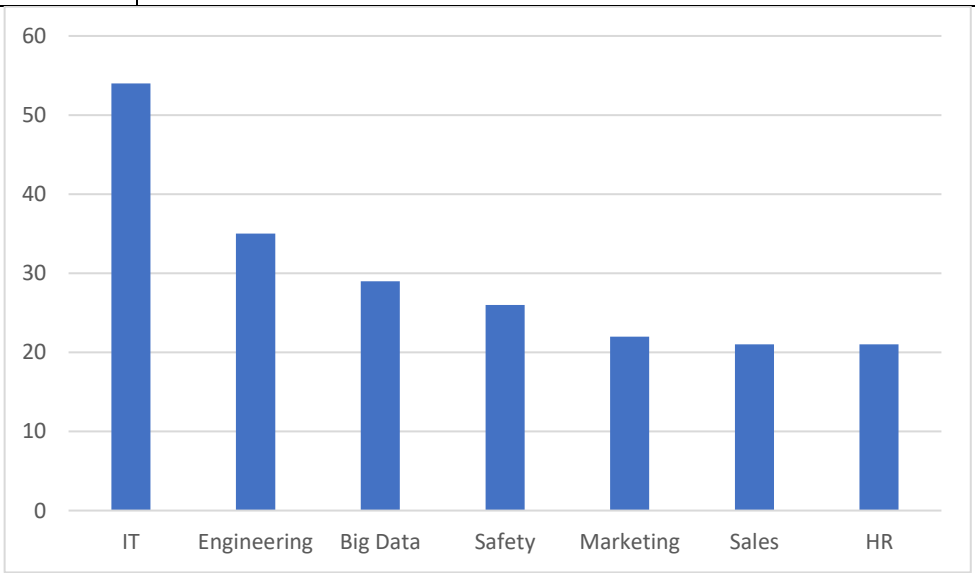


Graphic 6: Artificial Intelligence investment forecasts in the next year. Source: IBM Global AI Adoption Index.

The introduction of artificial intelligence has led to an incredible technological evolution of all sectors, not even sparing the labor market, imposing new scenarios: there has been a change in the skills required for human resources as well as the birth of new professions. The most requested workers are programmers, computer engineers, data scientists, who have found an increase in the demand for work.

Table 1: The most requested professional figures in the world of work.

54%	IT professionals
35%	Data engineers
29%	Developers and a data scientists
26%	Security professionals
25%	Customer service professionals
23%	Marketing professionals
21%	Product managers
21%	Sales professionals
21%	HR professionals
21%	Finance professionals

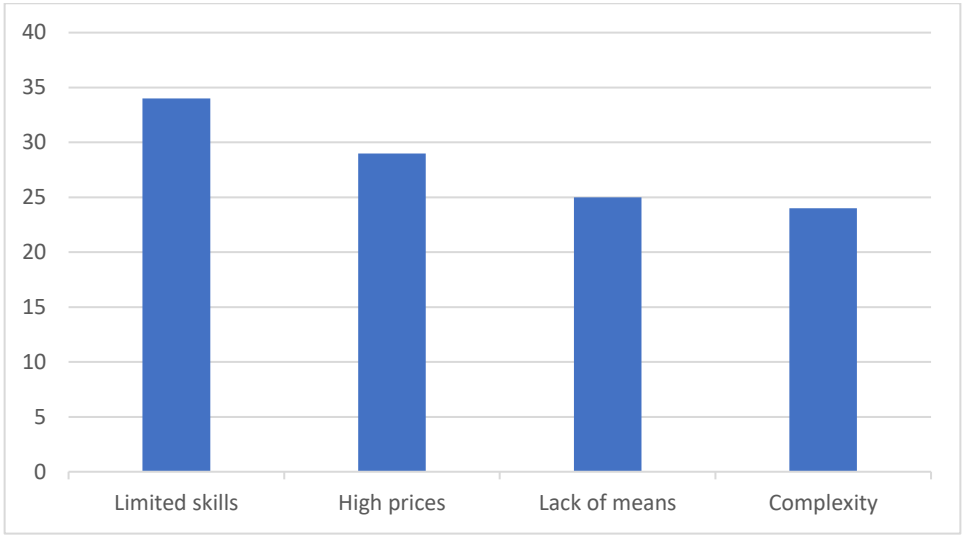


Graphic 7: Most important professional fields for the development of Artificial Intelligence. Source: IBM Global AI Adoption Index.

The survey also highlighted the main elements that determine an obstacle to the development of artificial intelligence for many companies: a relevant aspect concerns an element that is inherent in the

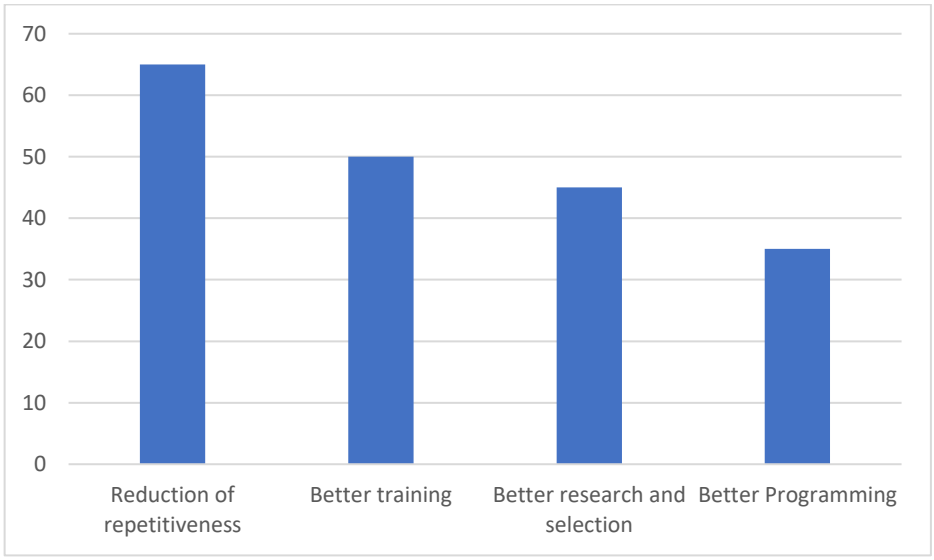
implementation of artificial intelligence which consists in its complex nature; in fact, many companies fail to take full advantage of the innovative approach so as to determine the failure of many activities carried out.

The primacy, however, concerns the limited technical skills, in fact it emerges that human resources are not adequately qualified, this is due to the excessive costs of training or the lack of material means that determine significant job gaps.



Graphic 8: Barriers that limit the development of Artificial Intelligence. Source: IBM Global AI Adoption Index.

Seen from another perspective, AI can represent a valid support for the management of the human resources sector, not only in the training of highly specialized personnel, also in the search and selection of professionals suitable for the reference area as well as in the planning of needs. of human resources.



Graphic 9: Fields of application of Artificial Intelligence in the management of human resources. Source: IBM Global AI Adoption Index.

The survey just analyzed shows the incidence of artificial intelligence technology in countries around the world and in the various multidisciplinary and application sectors.

It represents a fundamental element to build a position of competitive advantage such as to determine an "unbridgeable gap" for countries, organizations, companies, companies that will not invest in this technology.

The observed data reveal the decisive role of AI in recent years in the significant economic, cognitive and development growth of companies at an international level.

The results highlighted give good hope that investments in this science will lead to a significant prospect of generalized improvement for the near future.

2.3 Theoretical framework and history of AI

The fundamental elements[17], which form the basis of the operation of artificial intelligence are the concepts of agent, environment and actuators:

- the agent is intended as a rational agent as an element that processes the data acquired by means of special sensors (cameras, infrared, motion sensors);
- the environment represents the context in which the agent is operating;
- through the actuators the rational agent puts the actions into being.

The technical functioning of the artificial intelligence mechanism can be represented by a precise process:

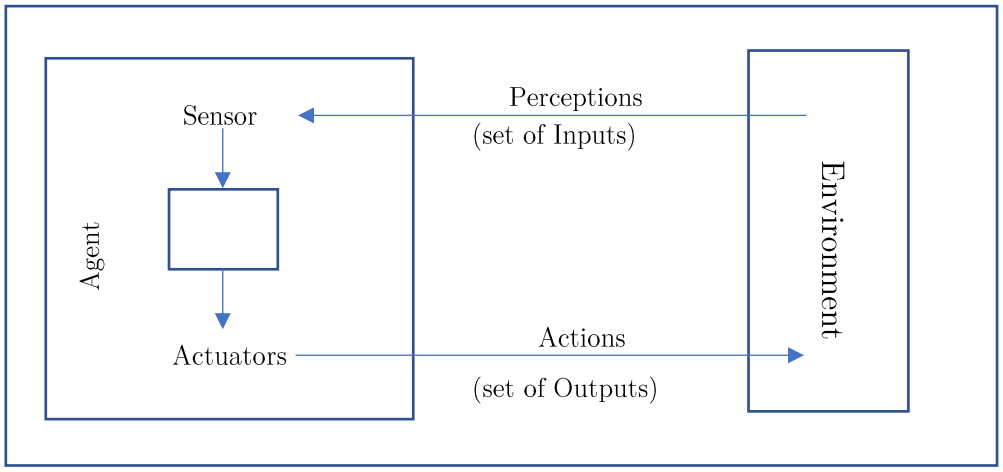


Figure 8: Artificial intelligence structure.

[17]Russell, SJ, & Norvig, P. (2005). Artificial intelligence. A modern approach (Vol. 1). Pearson Italia Spa.

The special sensors detect the set of perceptual inputs that are processed by the agent in order to generate an output intended as a set of actions implemented through the actuators. From the interaction of the elements just described, a characteristic element emerges, perception, it is the observation and analysis of the sets of inputs captured from the external environment with respect to which the agent carries out the actions. The authors Russel and Norvig define the agent as rational "who chooses the action that maximizes the expected value of his measure of performance, given the information provided by the perceptual sequence and any further knowledge of the agent".

Therefore, the role of the information extracted from the observed environment is fundamental, and this also depends on the different context in which the agent operates; in fact, it is possible to distinguish different types of environments. The completely observable environment is differentiated from a partially observable environment, in the first case it is possible to access all the elements, states and information at any time; in the second hypothesis there is the presence of limits that prevent the sensors from detecting the totality of perceptions. If the agent knows or does not know the laws underlying the environment, the known environment differs from the unknown one. The stochastic environment is characterized by elements of uncertainty, while in the absence of the latter the environment is considered deterministic. Further distinction is between the sequential environment, for which each action is influenced by the previous ones; with respect to the episodic environment in which the relevant elements are found at accurate moments for which the actions are a consequence only of perceptions of the observed instant. Furthermore, when every action is influenced by the continuous change of the context

we speak of a dynamic environment, otherwise the environment is defined as static. Finally, based on the values assumed by all the elements that come into play in the artificial intelligence mechanism, therefore data, information, input, time, actions it is possible to distinguish the discrete environment from the continuous one.

The introduction of "intelligent technologies" within an organization makes it possible to achieve important objectives in terms of productivity and competitive advantage, artificial intelligence represents a decisive technological evolution to obtain a significant positive impact not only on the individual organization, determining organizational and managerial development more efficiently and faster, but in general on the whole economy.

The first applied and commercialized approach of artificial intelligence was aimed at the decision making sector, through the design of systems that through specific algorithms were able to inspect a large amount of data to extract useful information for the management information system. The main objective was to improve the decision-making process of companies with computer programs that carried out the work of solving complex problems hitherto carried out by human experts[18].

The expression of artificial intelligence has only been introduced since 2000, the term used up to that moment was Expert system (Lu and Mooney, 1989; Dugdale, 1996; Dhaliwal and Tung, 2000) but the basic concept always remained the same. that is, IT systems to support the decision-making process.

---

[18]Durkin, 1996; Moody, Blanton and Will, 1998; Edwards, Duan and Robins, 2000.

Through an analysis of the literature, the origin of artificial intelligence can be traced back to 1950, when the scientist Alan Turing published the article Computing Machinery and Intelligence Turing in 1950[19]within which he believes that the operation of a machine can be traced back to "intelligent behavior" if it passes a certain test: the scientist, based on the "imitation game", formulates a three-participant test (Turing Test) in which a man in separate offices is confronted with two entities, another individual and a machine. Through a series of questions the man must identify if he interacts with the individual or with the machine, in the event that man is unable to make this distinction then the machine can be defined as intelligent since it is comparable to a human being. Furthermore, within the article by Turing emerges the expectation of creating systems capable of emulating human cognitive functions, and therefore the future artificial intelligence.

A significant previous contribution to the Turing test for the development of artificial intelligence was made by authors Warren McCulloch and Walter Pitts McCulloch[20], which laid the foundations of a neural network model inspired by the biological functioning of the human brain. These systems were composed of artificial neurons interconnected with each other, and which can assume the on or off state. According to this vision, the neuron represents the basic logical unit of the turing machine.

---

[19]Turing, AM, & Haugeland, J. (1950). Computing machinery and intelligence. The Turing Test: Verbal Behavior as the Hallmark of Intelligence, 29-56.

[20]McCulloch, WS, & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. The bulletin of mathematical biophysics, 5 (4), 115-133.

In 1951 the first neural network computer was developed by Marvin Minsky which was called SNARC, consisting of a network with 40 neurons.

Artificial intelligence thus registers ever greater interest: a significant date is 1956, the first academic conference is organized in Dartmouth college Hannover New Hampshire in this sector where many researchers gathered to discuss this topic. It is in this conference that the term artificial intelligence was born for the first time (McCarty et al.1955): "Every aspect of intelligence can be described in terms so rigorous as to make it possible to program a machine capable of simulating them". The first Logic Theorist artificial intelligence program is also presented. Conceived by the team of researchers led by Newell and Simon. the Logic Theorist was composed of a tree where the nodes were mathematical hypotheses able to solve precise mathematical theorems. This program was further developed by the same researchers. In 1957 they introduced the General Problem Solver: The initial program had been implemented the inferential process that simulated actions similar to human ones. At IBM, Gelernter realizes the Geometry Theorem Prover capable of proving geometric theorems.

the so-called Pandemonium was subsequently introduced, its production can be traced back to Oliver Selfridge in the Lincoln laboratory, its success is due to the fact that it is considered the first pattern recognition program, composed of functions trained to recognize precise objects in a written letter.

But to obtain the first complete model of artificial intelligence, it is necessary to wait until 1958 when McCarthy introduces the advice taker in his article Programs with Command Sense (McCarthy, J. (1959). Programs with common sense. Computer Science Department Stanford

University) a program that through the elaboration of sentences in formal language was able to interact with the surrounding environment.

In the field of pattern recognition, according to the American psychologist Rosenblatt, the neural network structure represents the best tool for this aspect; in particular the author in 1962 introduces the concept of perceptron, a model that presents a better neural network algorithm.

The first negative response to scientific research in the field of artificial intelligence was recorded with the implementation of automatic translation methods, Natural Language processing, the first attempts led to bad results so much as to lead the American government to suspend investments in research in this direction. Various criticisms followed against the new technology which until then had seen important growth prospects, underlining the failures of AI in those years. Hubert Dreyfus wrote the book "What computers can't do"[21].

After this period of failure in 1976 Weizenbaum created a program that replaces a psychologist called ELIZA: it was found a greater propensity on the part of patients to interact with the computer.

While until now the programs of artificial intelligence were part of the systems based on reasoning, starting from 1965 another school of thought was developed in particular, we go to study and introduce knowledge-based artificial intelligence systems. DENDRAL represents the first program based on the new approach, Designed by Edward Feigenbaum, capable of mapping the structure of a molecule through its spectral analysis.

[21]Dreyfus, HL (1992). What computers still can't do: A critique of artificial reason. MIT press.

Feigenbaum himself together with Buchanan created the best known of the expert systems, called MYCIN: It is a support model for doctors useful for diagnosing infectious blood diseases, based on medical knowledge and information relating to patients' symptoms.

in the 1980s, there was a growing interest in the industrial field of systems based on artificial intelligence. In 1982, Digital Equipment Corporation, a pioneering American company in the IT field, implemented R1, a system that allowed the hardware components of a computer to be configured, saving the company about $ 40 million per year.

the following years are characterized by strong enthusiasm for the implementation of expert systems in various sectors. The last twenty years have seen an acceleration in the progression of these systems: in the 2000s a decisive contribution was provided by the availability of databases in various areas, such that the implementation of knowledge-based systems is more laborious than in the past. (characterized by the manual insertion of all the necessary data), but we have moved towards the simplification of the procedures, through special learning algorithms the program relies on existing databases; and greater efficiency by being able to refer to a vast amount of data.

2.4 Different approaches of Artificial Intelligence

Artificial intelligence despite its development falls into various sectors, various disciplines, with different application elements between them, its functioning can be mainly traced back to four functions: listening, understanding, interaction, learning.

If the algorithm aims to classify and organize the data, we refer to the listening function. If, in addition to the classification and organization of data, the artificial intelligence algorithm is able to relate such data, helping the decision maker to have relevant information to make decisions, in this case the artificial intelligence performs the function of understanding. interaction is a specific function based on the exchange of information between artificial intelligence algorithms and the individual. Furthermore, algorithms can be implemented to learn through data analysis, this feature is the basis of learning: the more data we provide to the algorithm the better the result in terms of performance.

Within the discipline of artificial intelligence it is also possible to identify two types of approaches:

2.4.1 Weak Artificial Intelligence (ANI)

The restricted approach of artificial intelligence makes it possible to create machines capable of performing complex actions by simulating the modus operandi of man but not in a completely autonomous way, therefore the supervision of the individual is necessary. in this context the machine has an instrumental and support role to human activity and is very useful since it is a very powerful system; in fact, they have the ability to carry out actions in a shorter time than the human being, resulting in a tool of wide application use in many sectors.

2.4.2 Strong Artificial Intelligence (AGI)

This approach aims to create machines that are as autonomous as possible from human supervision, therefore these are systems that are able to solve a problem according to the mental scheme of man without being pre-programmed. these are possible through rules that indicate the procedure to be followed, the implementation of inferential mechanisms to

process the different situations thanks to the skills inherent in the system and through the user interface to make human use more friendly.

2.4.3 The super artificial intelligence

The research aims at the realization in the future of intelligent systems that go beyond the capabilities and understanding of man. At the base of this further approach are identified the impressive mnemonic capacity and the great speed of processing data as driving elements for the progress of super intelligent systems beyond humans in every field of knowledge.

2.5 Algorithms and learning models

Artificial intelligence represents a macro discipline that includes different subclasses: Machine Learning, Artificial Neural Networks, Deep learning, Natural Language processing.

The concept of machine learning was born in 1959 by the computer scientist Arthur Samuel when he worked at IBM, and can be defined as that branch of computer science that allows "machines to learn", that is, to acquire new knowledge through "reading keys" that man provides to the computer, which by means of algorithms is able to interpret the data available.

We therefore consider systems that use data learning algorithms to generate new knowledge and make predictions on the basis of this; therefore, it is useful to underline that the machine learning models systems are not programmed explicitly but proceed by "training".

Machine learning using machine learning is divided into four macro categories: supervised, unsupervised, reinforced and semi-supervised learning.

The type most used by organizations is supervised learning. This type of learning creates a prediction model of the target variable as a function of the predictive variables, that is, known data are available. In detail, the machine learns by using tagged data to learn how to predict an output value. Within this learning category and based on the output it is possible to distinguish the techniques: regression and classification. If the target variable is continuous then regression will be used, in case of discrete target variable the technique to implement will be the classification.

Unsupervised learning takes the form of the technique of looking for patterns from unlabeled data to extract unknown information. In this case the machine learns without knowing the output but only through the input data for this reason it is more complex than the previous category. The techniques that fit into the unsupervised learning category are clustering and size reduction. If the objective of the analysis is the subdivision into groups of the input data, we use the clustering technique which consists in the exploration of data in the absence of information with respect to the relationships existing between the same data, to carry out groupings in clusters through the identification of similar characters. In the'

A hybrid technique and semi-supervised learning that is more suitable in the hypothesis in which the classification of the data has the character of imprecision or are wrong, or in case of loss of the labels.

Learning with reinforcement is achieved through a process called trial and error, this process consists in assigning the system a penalty or a reward according to the correctness of the action performed, the procedure is repeated until the resolution of the problem that maximizes the reward total (output).

Artificial neural networks fall within the category of machine learning. As the name of this further application of artificial intelligence emerges, it is a system that assumes the structure of a comma human brain as it is made up of millions of artificial neurons connected to each other.

In detail, the structure of a neural network is divided into input units, hidden layers and output units. The operation consists of a first phase of acquisition of information by the input units which transmits them to the hidden layers formed by different neurons within which we proceed to the processing of information and the learning of the bonds between the various neurons up to arrive at the association of actual outputs.

The accuracy of a neural network depends on the number of neurons that compose it and on the synaptic connections between them, for this reason the redundancy of elements that make up the overfitting network or the reduced or insignificant use of over-training examples; can affect the accuracy of the model.

The most used type of artificial neural networks is feed-forward which is characterized by the presence of an input layer, one or more hidden layers and an output layer; in this model each of the neurons is connected with

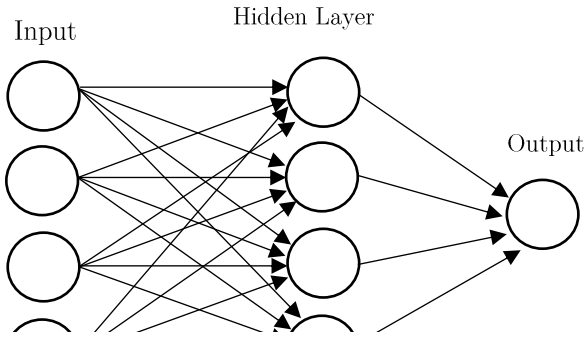


Figure 9: Architecture of an Artificial Neural Network.

all those of the previous layer but is devoid of connections with the neurons of the same layer and the signal is unidirectional that is it propagates from the input to the hidden layers up to the output.

The network architecture determines how the signal is processed, based on the classical architecture and considering a single hidden layer, the expression that allows us to identify the relationship between the input vector and the value of the output variable is the following:

$$y = g\left[\beta_0 + \sum_{m=1}^{M} \beta_m \phi\left(\alpha_{0m} + \sum_{i=1}^{d} a_{im} x_i\right)\right] + \varepsilon \tag{3.1}$$

Where is it:

y= output variable

g= transformation function (hidden units→output)

β_0= output related bias

β_m= weight of the hidden unit link and output value

ϕ= transfer function (input→hidden units)

α_{0m}= bias related to hidden drives

a_{im}= weight connected between inputs and hidden units

x_i= input vector

ε= random variable

The fields of application of artificial neural networks are different. It is a useful tool in marketing to segment the target audience of a company by considering multiple variables such as income, purchases, geographic location and so on. In the sales sector, it has the ability to advance forecasts to anticipate customer needs, thus obtaining a competitive advantage over

competitors. It is also possible to make forecasts about the performance of financial assets. To understand the extent and importance that such advanced technology has assumed, there is a validity in the medical sector for the prevention of diseases.

Based on neural networks is the so-called Deep Learning technology which consists of a machine learning system with multiple levels of abstraction. In this context, the machine learns from the enormous amount of data available and then processed by the neural networks; in this case the learning process is not required to be guided by a programmer. There are several application areas from object classification, to autonomous vehicles, from automatic translation machines to Sentiment Analysis.

Natural Language Processing is based on Deep Learning: this is technology to the ability to understand and interpret the natural language of man in order to perform certain tasks. tool widely used in the modern period whose application functions can be found in chatbots, in the marketing sector it allows to provide customer assistance 24 hours a day; sentiment Analysis with respect to which it is possible, for example, to extract useful information from comments, reviews on products and so on; through Natural Language processing it is possible to translate a text into different languages; in addition to the ability to process and interpret a large amount of data by creating comparative analyzes and reports.

3 Chapter: Decision making in a fuzzy environment

3.1 Introduction; 3.2 Fuzzy logic: expert systems; 3.3 Fuzzy Theory; 3.3.1 Fuzzy Set; 3.4 Membership functions; 3.4.1 Triangular membership function; 3.4.2 Trapezoidal membership function; 3.4.3 Concept of Support, Core and Height; 3.4.4 Fuzzy Singleton.

3.1 Introduction

Decision making means choosing one of several alternative ways of solving a problem. Often the decision maker has to make decisions based on qualitative information derived from personal observations. In other cases, it is based on synthetic evaluations drawn from masses of data, perhaps with an automatic data mining process. Decision making is therefore more difficult when dealing with incomplete, inaccurate and subjective information, i.e. when the information is fuzzy. Fuzzy sets are well suited to characterize the different types of information, allowing the explicit models otherwise tacit. Think, for example, of a strategic marketing decision in which the decision maker thinks in terms of high or low market receptivity, high or low price/production cost ratio, etc.

3.2 Fuzzy logic: expert systems

"Fuzzy expert systems are automatic methods that tend to reproduce the method of human reasoning, applied to specific problems."

Expert systems are types of decision-making computer software based on Boolean logic, which means that the system uses a series of yes or no answers to try to solve a problem.

The fuzzy expert system is a form of problem solving used by a computer system, often used in the creation of artificial intelligence. Such systems expand the operation of the traditional expert system and rely on fuzzy logic rather than boolean logic. With fuzzy logic, as discussed earlier, the computer must try to compute an answer based on answers that may not be completely true but may not be entirely false either.

Starting point: observing that in the real world, decision-making processes, or reasoning, always have the same goal, to find a relationship between input elements and output results.

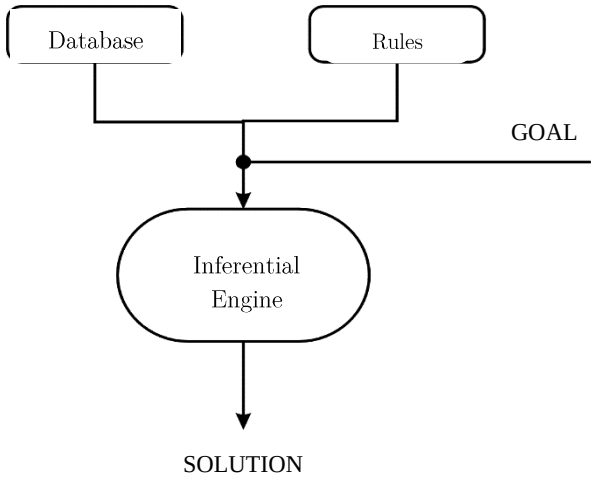


Figure 10: Structure of an expert system.

In this direction, computer research has proposed new paradigms and programming languages aimed at inferring new knowledge or data configurations starting from a database and constraints, which represent the rules seen previously.

3.3 Fuzzy Theory

The origin of Fuzzy Set Theory is marked by the publication in 1965 by the mathematical engineer Lofti A. Zadeh, of the article "Fuzzy Sets" in the journal Information and Control. The author sensed that the classes of objects encountered in the real physical world do not have well-defined membership criteria, thus laying the foundations for an approach related to classification problems by exploiting the notion of vague information, an approach that most reflects human reasoning in the resolution of problems. The goal of this new method is to arrive at a more precise description of the sets we encounter in real life.

Fuzzy theory was introduced by replacing the rigid membership relationship of ordinary set theory, based on the excluded third principle; the most flexible relationship that provides a degree of belonging of each object.

3.3.1 Fuzzy Set

The fuzzy set concept is formalized as follows.

Let X be a non-empty set, a fuzzy set A on the set X is defined as a set of pairs:

$$A = \{[x, f_A(x)]\} \tag{4.1}$$

Where x is the generic element of the set X, and f_A a real function, called membership function, whose defining set is X. The value $f_A(x)$ is called membership value or degree of membership of x in the fuzzy set A.

The value $f_A(x)$ reflects our (subjective) willingness to accept the element x as a member in A. The membership function f_A can assume values in the closed interval [0,1].

Therefore $f_A(x)$ can take the following values:

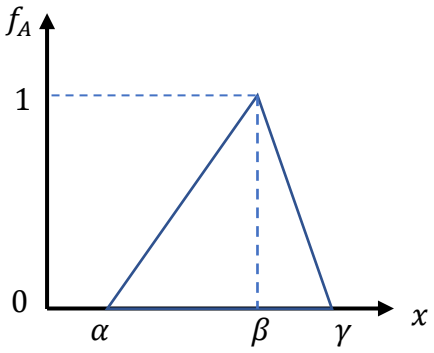
- $f_A(x) = 1 \rightarrow x$ definitely belongs to A (complete acceptance of x as a member);
- $f_A(x) = 0 \rightarrow x$ it does not belong to A (we reject x entirely);
- $0 < f_A(x) < 1 \rightarrow x$ partially belongs to A.

3.4 Membership functions

Depending on the type of application, very different membership functions can be defined. Considering a set A and a function f_A, the most used membership functions are:

3.4.1 Triangular membership function

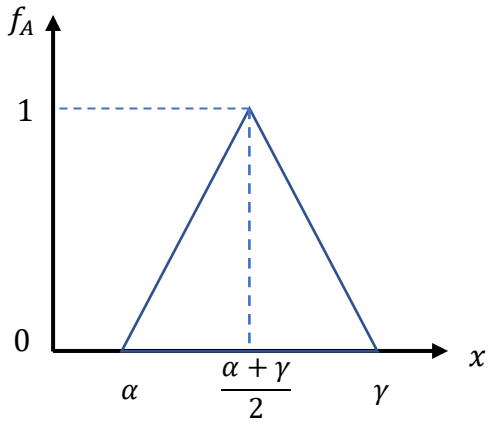
A triangular fuzzy number is typically denoted by three parameters: the extremes α and γ; and the maximum point β:



Graphic 10: Triangular fuzzy numbers.

$$f_A(\alpha,\beta,\gamma) = \begin{cases} 0 & x < \alpha \\ \dfrac{x-\alpha}{\beta-\alpha} & \alpha \le x \le \beta \\ 1 & x = \beta \\ \dfrac{\gamma-x}{\gamma-\alpha} & \beta \le x \le \gamma \\ 0 & x > \gamma \end{cases}$$

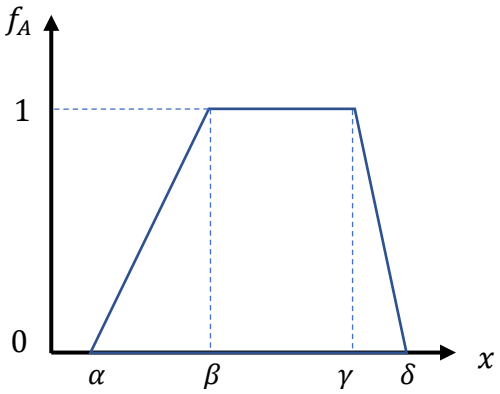
In practice it often results that $\beta = \frac{\alpha+\gamma}{2}$, that is, there is a central triangular fuzzy number represented graphically by the following membership function:



Graphic 11: Symmetrical fuzzy triangular graph.

3.4.2 Trapezoidal membership function

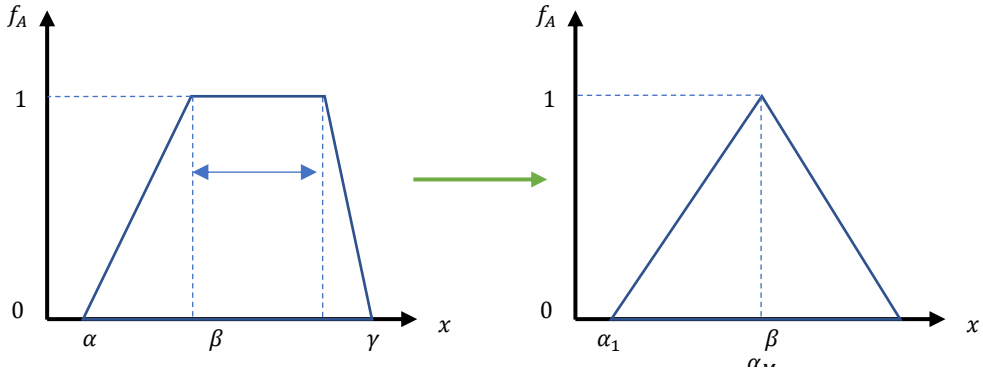
A trapezoidal fuzzy number is defined with four parameters: the extremes α and δ, the lower and upper values of the range of maximum β and γ.



Graphic 12: Trapezoidal fuzzy numbers.

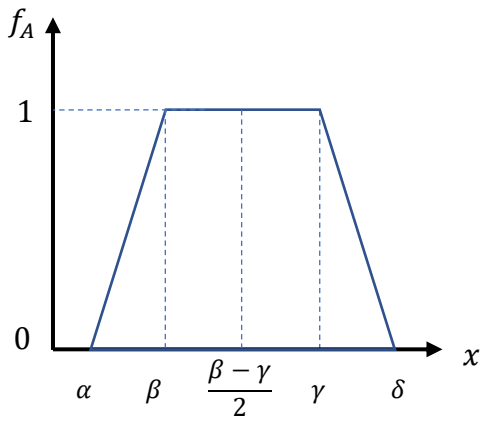
$$f_A(\alpha,\beta,\gamma,\delta) = \begin{cases} 0 & x < \alpha \\ \dfrac{x-\alpha}{\beta-\alpha} & \alpha \le x \le \beta \\ 1 & \beta \le x \le \gamma \\ \dfrac{\delta-x}{\delta-\gamma} & \gamma \le x \le \delta \\ 0 & x > \delta \end{cases}$$

If $\beta = \gamma$ the trapezoidal fuzzy number is traceable to the triangular fuzzy number denoted as follows: $f_A = (\alpha_1, \alpha_M, \alpha_M, \alpha_2)$.



Graphic 13: Triangular trapezoidal fuzzy numbers

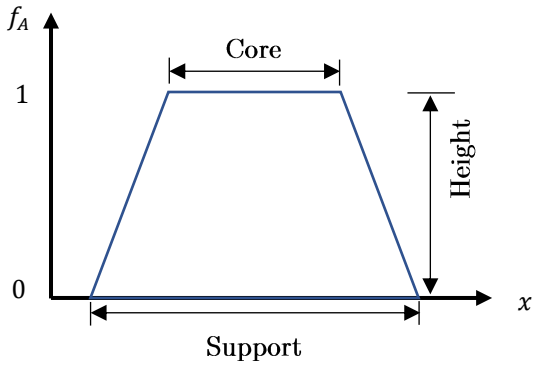
In practice this often results $[\alpha,\beta] = [\gamma,\delta]$ in a symmetrical trapezoidal number with respect to the straight line $x = \frac{\beta-\gamma}{2}$, defined as a central trapezoidal fuzzy number.



3.4.3 Concept of Support, Core and Height

Consider A a Fuzzy subset of X, the support of A is the subset of X

Graphic 14: Symmetrical fuzzy trapezoidal graphic.



Graphic 15: Core, Support and Height

consisting of all elements with non-zero degree of membership:

$$supp_{(A)} = \{x | f_A(x) > 0\}$$

The core of A is the subset of X containing the set of values such that the membership function of all elements is equal to 1:

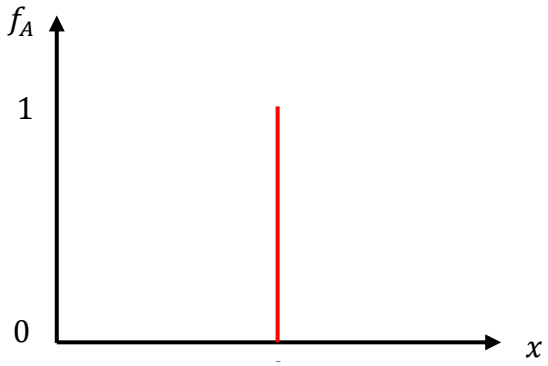
$$core_{(A)} = \{x | f_A(x) = 1\}$$

The height corresponds to the upper extreme:

$$Height_{(A)} = Sup_{x \in X}\, f_A(x)$$

3.4.4 Fuzzy Singleton

It is a set that has only one element in which the value of the membership function is equal to 1.



GraphicA: Fuzzy Singleton

4 Chapter: Hybrid Fuzzy Differential System and Artificial Neural Networks: Some Issues in Economics

4.1 Introduction; 4.2 The Hybrid Fuzzy Differential System: A New Model; 4.3 Neural Networks: New Issues; 4.4 Concluding Remarks and Further Developments in the Frame of Artificial Intelligence and Machine Learning.

4.1 Introduction

The work presented below represents a hybrid model of the tools examined in the previous chapters, especially with reference to the fuzzy environment and artificial neural networks.

In the recent years, fuzzy analysis and fuzzy differential equations were proposed to handle uncertainty due to incomplete information that appears in many mathematical or computer models of some deterministic real world phenomena. This theory has been further developed and a wide number of applications of this theory have been considered in the real-world systems. This theory is attractive because it is based on a very intuitive, although somewhat subtle, idea capable of generating many intellectually appealing results that provide new insights to old, often-debated questions.

Thereafter, the applications of this interesting theory are described in the mathematical modeling and show us the way to model the physical problems with fuzzy parameters. In the final step, some important numerical techniques are prescribed to solve fuzzy differential equations. Fuzzy differential equations (FDEs) are an interesting field of the analysis mathematics very useful for studying and solving large proportions of problems in many issue of applied mathematics, eg physics, geography, medicine, biology, control chaotic systems, bioinformatics and computational biology, synchronize hyperchaotic systems, economics and finance, and so on. See for instance Casasnovas et al. (2005), Feng and Chen (2005), Zhang et al. (2005). FDEs born in order to model the propagation of epistemic uncertainty in a dynamical environment. In fact FDEs are significant to model problems where the degree of ambiguity is high (Otadi et al. 2017). FDEs can be studied by several approaches. The Hukuhara differentiability for fuzzy number valued functions was the first approach which has been utilized. Fuzzy differential equations were first formulated by Kaleva (1987) and Seikkala (1987) in time dependent form. A very general formulation of a fuzzy first-order initial value problem, has been given by Buckley and Feuring (2000).

Hybrid systems evolve in continuous time, like differential systems, but undergoing a fundamental change in their governing equations at a sequence of discrete times. When a continuous time dynamics of a hybrid system is given by a FDE, the system is called a hybrid fuzzy differential system. For analytical results on hybrid fuzzy differential equations (HFDEs), see Lakshmikantham and Liu (1998) and Lakshmikantham and Mohapatra (2003). Hybrid systems are devoted for modeling, designing, and validating interactive systems of computer programs and continuous

systems as well. These control systems which are capable of controlling complex systems have discrete event dynamics as well as continuous time dynamics that can be modeled by hybrid systems.

In this work, we propose an approach to solve the hybrid fuzzy differential equations based on the feed-forward neural networks. This method shows that using neural networks provides solutions with good generalization and the high accuracy. To do this we shall briefly discuss the following subjects; Artificial neural networks (ANN), and FDEs. ANN are computing systems that are inspired by, but not identical to, biological neural networks that constitute animal brains. Such systems "learn" to perform tasks by considering examples, generally without programmed with taskspecific rules. FDEs are relevant to approach all the phenomena that need modeling with uncertain parameters. It gives us enough tools to model real-world system and approach us much closer to its behavior.

4.2 The Hybrid Fuzzy Differential System: A New Model

Consider the following hybrid fuzzy differential system:

$$\begin{cases} y'(x) = f\big(x, y(x), \lambda_k(y_k)\big), x \in [x_k, x_{k+1}] \\ y(x_k) = y_k \end{cases} \tag{4.1}$$

where $0 \leq x_0 < x_1 < \cdots < x_k < \cdots, x_k \to \infty, f \in C[R^+ \times E \times E, E], \lambda_k \in C[E, E]$

To be specific, the system would look like:

$$y'(x)=\begin{cases} y_0'(x)=f\big(x,y_0(x),\lambda_0(y_0)\big),y_0(x_0)=y_0, & x_0\le\ x\le\ x_1\\ y_1'(x)=f\big(x,y_1(x),\lambda_1(y_1)\big),y_1\ (x_1)=y_1, & x_1\le x\le x_2\\ \vdots & \vdots\\ y_k'(x)=f\big(x,y_k(x),\lambda_k(y_k)\big),y_k(x_k)=y_k\ , & x_k\le x\le x_{k+1}\\ \vdots & \vdots \end{cases} \tag{4.2}$$

Assuming that the existence and uniqueness of solutions of Eq. (4.1) hold for each $[x_k,x_{k+1}]$, by the solution of Eq. (4.1), we obtain the following function:

$$y(x)=y(x,x_0,y_0)=\begin{cases} y_0(x),x_0\le x\le x_1\\ y_1(x),x_1\le x\le \mathrm{x}_2\\ \vdots\\ y_k(x),x_k\le x\le x_{k+1}\\ \vdots \end{cases} \tag{4.3}$$

We note that the solutions of Eq. (4.1) are piecewise differentiable in each interval for $x\in[x_k,x_{k+1}]$, for a fixed $y_k\in E$ and $k=0,1,2,\dots$ We replace Eq. (5.1) by the following equivalent system:

$$\begin{cases} \underline{y'}(x)=\underline{f}\big(x,y(x),\lambda_k(y_k)\big),\underline{y}(x_k)=\underline{y_k}\\ \overline{y'}(x)=\overline{f}\ \big(x,y(x),\lambda_k\ (y_k)\big),\overline{y}(x_k)=\overline{y_k} \end{cases} \tag{4.4}$$

The parametric form of the above systems is given by:

$$\begin{cases} \underline{y'}(x,r)=F\left(x,\underline{y}(x,r),\overline{y}(x,r),\underline{\lambda_k}(y_k)(r),\overline{\lambda_k}(y_k)(r)\right),\underline{y}(x_k\ ,r)=\underline{y_k}(r)\\ \overline{y'}(x,r)=G\left(x,\underline{y}(x,r),\overline{y}(x,r),\underline{\lambda_k}(y_k)(r),\overline{\lambda_k}(y_k)(r)\right),\overline{y}(x_k\ ,r)=\overline{y_k}(r) \end{cases} \tag{4.7}$$

where $x \in [x_k, x_{k+1}]$ and $r \in [0,1]$. Using Bede's characterization theorem proposed by Bede (2008), Pederson and Sambandham (2009) generalized the following characterization theorem for HFDEs.

Theorem 1: Consider the HFDE (4.1) expanded as Eq. (4.2) where for $k = 0, 1, 2, \ldots$ and each $f_k: [x_k, x_{k+1}] \times E \to E$, we have:

1. $[f_k(x,y)]^r = \left[\underline{f}_k^r\left(x, \underline{y}, \overline{y}\right), \overline{f}_k^r\left(x, \underline{y}, \overline{y}\right)\right]$;

2. $\underline{f}_k^r$ and $\overline{f}_k^r$ are equicontinuous and uniformly bounded on any bounded set;

3. There exists a $L_k > 0$ such that

$$\left|\underline{f}_k^r(x,y,z) - \underline{f}_k^r(x,y_1,z_1)\right| \leq L_k max\{|y_1 - y|, |z_1 - z|\} \; for \; all \; r \in [0,1]$$

$$\left|\overline{f}_k^r(x,y,z) - \overline{f}_k^r(x,y_1,z_1)\right| \leq L_k \max\{|y_1 - y|, |z_1 - z|\} \; for \; all \; r \in [0,1]$$

Then, the FIVP (Eq. 5.1) and system of ODEs:

$$\begin{cases} \underline{y}_k^r(x)' = \underline{f}_k^r\left(x, \underline{y}_k^r, \overline{y}_k^r\right) \\ \overline{y}_k^r(x)' = \overline{f_k^r}\left(x, \underline{y}_k^r, \overline{y}_k^r\right) \\ \underline{y}_k^r(x_k) = \underline{y}_{k-1}^r(x_k), \quad if \; k > 0, \underline{y}_0^r(x_0) = \underline{y}_0^r \, r \\ \overline{y}_k^r(x_k) = \overline{y}_{k-1}^r(x_k), \quad if \; k > 0, \overline{y}_0^r(x_0) = \overline{y}_0^r r \end{cases}$$

are equivalent.

4.3 Neural Networks: New Issues

Using neural networks provides solutions with very good generalizability (such as differentiability). However, an important future of multilayer perceptrons is their utility to approximate functions, which leads to a wide applicability in most problems.

In this article, the function approximation capability of feed-foreword neural networks is used by expressing the trial solution for system (4.7) as the sum of two terms (see Eq. 4.6). The first term satisfies the initial conditions and does not contain adjustable parameters. The second term involves a feed-forward neural network to be trained, so satisfies the differential equations. Since it is known as a multilayer perceptron with one hidden layer which can approximate any function to arbitrary accuracy, the multilayer perception is used as the type of the network architecture.

If $\underline{y}_T\left(x,r,\underline{p}\right)$ corresponding networks is a trial solution for the first equation in system (1) and $\overline{y}_T(x,r,\overline{p})$ is a trial solution for the second equation in system (1) where $\underline{p}$ and $\overline{p}$ are adjustable parameters (indeed $\underline{y}_T(x,r,\overline{p})$ and $\overline{y}_T(x,r,\overline{p})$ are approximations of $\underline{y}_T(x,r)$ and $\overline{y}_T(x,r)$ respectively), then a discretized issue of system (1) might be converted to the optimization problem.

$$\min_{\vec{v}} \sum_{i=1}^{m} \Big\{ \Big(\underline{y'}_T(x_i, r, \underline{v}) - F\left[x_i, \underline{y}_T(x_i, r, \overline{v}), \overline{y}_T(x_i, r, \overline{v}), \overline{\lambda}_k(y_k)(r), \overline{\lambda}_k(y_k)(r)\right]\Big)^2 + \big(\underline{y'}_T(x_i, r, \overline{v}) - G\left[x_i, \overline{y}_T(x_i, r, \underline{v}), \overline{y}_T(x_i, r, \overline{v}), \underline{\lambda}_k(y_k)(r), \overline{\lambda}_k(y_k)(r)\right]^2 \Big\} \tag{4.5}$$

Were $\vec{v} = \left(\underline{v}, \overline{v}\right)$ includes all adjustable parameters with the initial conditions

$$\underline{y}_T(x_0, r, \underline{v}) = \underline{y}_0(r), \qquad \overline{y}_T(x_0, r, \overline{v}) = \overline{y}_0(r)$$

Each trial solution $\underline{y}_T$ and $\overline{y}_T$, employs one feed-forward neural network forwhich the corresponding networks are denoted by $\underline{N}$ and $\overline{N}$, with adjustable parameters $\underline{v}$ and $\overline{v}$, respectively. Thus, $\underline{y}_T$ and $\overline{y}_T$ can be selected as follows:

$$\begin{aligned}\underline{y'}_T(x,r,\underline{v}) &= \underline{y}(x_0,r) + (x-x_0)\underline{N}(x,r,\underline{v})\\ \overline{y'}_T(x,r,\overline{v}) &= \overline{y}(x_0,r) + (x-x_0)\overline{N}(x,r,\overline{v})\end{aligned} \tag{4.6}$$

where $\underline{N}$ and $\overline{N}$ are single-output feed-forward neural networks with adjustable parameters $\underline{v}$ and $\overline{v}$, respectively. Here, x and r are the network inputs. It is easy to see that in Eq. (4.6), $\underline{y}_T$ and $\overline{y}_T$ satisfy the initial conditions. From Eq. (4.6), it is easy to show that:

$$\begin{cases}\underline{y'}_T(x,r,\underline{v}) = \underline{N}(x,r,\underline{v}) + (x-x_0)\dfrac{\delta \underline{N}}{\delta x}\\ \underline{y'}_T(x,r,\overline{v}) = \overline{N}(x,r,\overline{v}) + (x-x_0)\dfrac{\delta \overline{N}}{\delta x}\end{cases} \tag{4.7}$$

Now suppose a multilayer perceptron has a hidden layer with H sigmoid units and a linear output unit. Therefore, we have:

$$\begin{cases}\underline{N} = \sum_{i=1}^{m} \underline{w_i}\sigma\left(\underline{t_i}\right), & \underline{t_i} = \underline{a}_{i1}x + \underline{a}_{i2}x + \underline{b_i}\\ \underline{N} = \sum_{i=1}^{m} \overline{w_i}\sigma(\overline{t_i}), & \overline{t_i} = \overline{a}_{i1}x + \overline{a}_{i2}x + \overline{b}_i\end{cases} \tag{4.8}$$

were $\sigma(t)$ is the sigmoid transfer function, $\underline{a}$ and $\overline{a}$ ($m \times 2$ matrices) are the weights of input layers, and $\underline{b}$ and $\overline{b}$ ($m \times 1$ matrices) are the bias vectors of input units $\underline{w}$ and $\overline{w}$ ($m \times 1$ matrices) are the weight vectors of

output units, and $\sigma(t) = \frac{1}{1+e^{-t}}$ is the sigmoid transfer function. The following is obtained:

$$\begin{cases} \dfrac{\partial \underline{N}}{\partial x} = \displaystyle\sum_{i=1}^{m} \underline{w}_i \, \underline{a}_{i1} \sigma'(\underline{t}_i) \\ \dfrac{\partial \overline{N}}{\partial x} = \displaystyle\sum_{i=1}^{m} \overline{w}_i \, \overline{a}_{i1} \sigma'(\overline{t}_i) \end{cases} \tag{4.9}$$

where $\sigma'(\overline{t}_i)$ is the first derivative of the sigmoid function. Now, if we substitute Eq. (5.7) in (5.5), the constrained optimization problem (5.5) might be changed with the unconstrained optimization problem as follow:

$$\min_{\vec{v}} \sum_{i=1}^{n} \begin{cases} \left(\underline{N}(x, r, \underline{v}) + (x - x_0)\dfrac{\delta \underline{N}}{\delta x} - F[x_i, \underline{y}_T(x_i, r, \underline{v}), \overline{y}_T(x_i, r, \overline{v}), \underline{\lambda}_k(y_k)(r), \overline{\lambda}_k(y_k)(r)]\right)^2 + \\ +\left(\underline{N}_T(x_{i1}, r, \overline{v}) + (x_i - x_0)\dfrac{\delta \overline{N}}{\delta x} - G[x_i, \underline{y}_T(x_i, r, \underline{v}), \overline{y}_T(x_i, r, \overline{v}), \underline{\lambda}_k(y_k)(r), \overline{\lambda}_k(y_k)(r)]\right)^2 \end{cases} \tag{4.10}$$

4.4 Concluding Remarks and Further Developments in the Frame of Artificial Intelligence and Machine Learning

By this ongoing research we have to show a new method for solving HFDEs. We try introducing the reader to understand the ability of neural networks for approximating the solutions of FDEs. By comparing our achievements with the results obtained using numerical methods, it is clear that our proposed method gives more accurate approximations. Applicability in function approximations of neutral networks is the main reason for using neural networks. More research is in progress for applying and extending this new approach for solving nth-order FDEs as well as a system of FDEs.

In this fascinating direction of research we are going to explore the application of this mathematical platform in the frame of Artificial intelligence and Machine Learning. This is the natural extension of the present work. In summary, we defined a new method for solving HFDEs. We demonstrated the ability of neural networks for approximating the solutions of FDEs. By comparing our achievements with the results obtained using numerical methods, it is clear that our proposed method gives more accurate approximations. Also better results (specially in nonlinear cases) might be possible if we use more neurons or training points. In addition, after solving a FDE, we obtained the solution at any arbitrary point in the training interval (even between training points). Applicability in function approximations of neutral networks is the main reason for using neural networks. More research is in progress for applying and extending this new approach for solving nth-order FDEs as well as a system of FDEs. The numerical results showed that the method has good accuracy and it is efficient summary, we defined a new method for solving HFDEs. We demonstrated the ability of neural networks for approximating the solutions of FDEs. By comparing our achievements with the results obtained using numerical methods, it is clear that our proposed method gives more accurate approximations. Also better results (specially in nonlinear cases) might be possible if we usemore neurons or training points. In addition, after solving a FDE, we obtained the solution at any arbitrary point in the training interval (even between training points). When we talk about Artificial Intelligence, we immediately think of cutting-edge technologies, robots that can understand and decide what actions to take and a futuristic world in which machines and men live together. In reality, Artificial Intelligence, and its use are much more real than we can imagine

and now used in different areas of daily life. In technical terms, Artificial Intelligence is a branch of Computer Science that allows the programming and design of both hardware and software systems that allow machines to be equipped with certain characteristics that are typically considered human, such as visual, spatio-temporal and decision-making perceptions. In fact, an intelligent system is created by trying to recreate one or more of these different forms of intelligence which, although often defined as simply human, can actually be traced back to particular behaviors reproducible by some machines. Starting from the brain work, Artificial Intelligence should be able to perform some human functions, such as: spatio-temporal and decision-making perceptions. In fact, an intelligent system is created by trying to recreate one or more of these different forms of intelligence which, although often defined as simply human, can actually be traced back to particular behaviors reproducible by some machines. In particular, Artificial Intelligence should be able to perform some human functions, such as:

- act humanly (that is, in an indistinct manner with respect to a human being)
- think humanly (solving a problem with cognitive functions)
- think rationally (that is, using logic as a human being does)
- act rationally (starting a process to obtain the best expected result based on the information available, which is what a human being, often even unconsciously, makes a habit of).

These considerations are very important because they allow us to classify the AI into two great "strands": the weak AI and the strong AI. The weak formulation claims that a computer will never be able to be equivalent to a human mind, but will only be able to simulate some of the cognitive

processes humans without being able to reproduce them in their total complexity. According to the weak setting, the design of smart programs is just a tool to verify theories about how humans could perform cognitive operations. The final purpose of this theory is the construction of machines able to exhibiting behaviors that they would be considered intelligent like humans. The strong formulation believes that a properly programmed computer can be truly endowed with a pure intelligence, not distinguishable in any way from human intelligence. The idea behind this theory is the concept that goes back to the philosopher English empiricist Hobbes, who argued that "reasoning is nothing else than calculating". The human mind would therefore be the product of a complex set of calculations performed by the brain. According to this conception, a computer properly programmed is a real mind, in the sense that it can be said that the computers in which they were introduced adequate programs understand and have real cognitive states. The debate on the strong formulation of artificial intelligence raises some of the most difficult conceptual problems of all philosophy. It is perfectly consistent to believe that it is impossible to build machines capable of acting in clever way, but be willing not to recognize such machines in full consciousness if it could be built.

5 Chapter: Exponential Increment of RSA Attack Range via Lattice Based Cryptanalysis

5.1 Introduction; 5.2 Preliminaries; 5.2.1 Lattice Reduction; 5.2.2 Coppersmith's method; 5.3 The Proposed Attack on RSA; 5.4 Comparison with Existing Results; 5.4.1 Comparison with the result in Boneh-Durfee's work; 5.4.2 Comparison with the result in Kumar-et al.'s work; 5.4.3 Comparison with the result in Blomer-May's work; 5.4.4 Comparison with the result in Bunder-Tonien's work; 5.4.5 Comparison with the result in Ariffin-et al.'s work. 5.4.6 A numerical example; 5.5 Conclusion.

5.1 Introduction

The fundamental resource of the decision-making process is the data, as basic elements to elaborate a careful analysis of the results, in order to obtain possible insights useful for the elaboration of competitive strategies. For this reason, data security at any level of an organization in the industry is of enormous importance.

In this scenario, cryptanalysis plays an important role in the decision-making processes. The significant contribution to cryptoanalysis was recorded by Alan Turing, founder of modern computer science, who decided on the cryptographic system enigma. Worthy of consideration was the

COLOSSUS, a hardware device for decrypting cryptographic systems to be considered the precursor of modern digital computers.

The encryption techniques make it possible to protect data, information, documents especially in the transmission phase by means of a telematic network in the work they present themselves.

The work presents an analysis of the RSA connection system within which we will try to provide valid demonstrations about the choice of the exponent and private to ensure that the cryptosystem is invulnerable from attacks.

The RSA cryptosystem comprises of two important features that are needed for encryption process known as the public parameter e and the modulus N. In 1999, a cryptanalysis on RSA which was described by Boneh and Durfee focused on the key equation $ed - k\phi(N) = 1$ and e of the same magnitude to N. Their method was applicable for the case of $d < N^{0,292}$ via Coppersmith's technique. In 2012, Kumar et al. presented an improved Boneh-Durfee attack using the same equation which is valid for any e with arbitrary size. This paper presents an exponential increment of the two former attacks using the variant equation $ea - \phi(N)b = c$. The new attack breaks the RSA system when a and $|c|$ are suitably small integers. Moreover, the new attack shows that the Boneh-Durfee attack and the attack of Kumar et al. can be derived using a single attack. We also showed that our bound also manage to improve the bounds of Ariffin et al. and Bunder and Tonien.

The initial idea of cryptography started from a symmetric idea which implies that users were utilizing the same key in order to encrypt and decrypt the data. However, the problem on how to distribute key efficiently eventually arose as the number of the users increased. Two cryptographers

namely Diffie and Hellman contributed towards solving this problem by introducing public key cryptography (PKC) or also known as asymmetric cryptography which lead to a successful mass utilization of cryptography[22]. An important feature of PKC is that, it uses a one-way function together with its trapdoor information. A one way function is a function that is easy to compute but computationally infeasible to invert unless if one has the trapdoor information that allows the inverse computation in polynomial time[23]. In 1978, Rivest, Shamir, and Adleman used the idea of Diffie and Hellman and invented an astounding cryptosystem namely RSA [24]and it has been deployed globally to provide security in communication as well as protect information. The main characters in the RSA are the modulus N where it is a product of two distinct large and balance primes called p and q, a parameter e which is set as public key and relatively prime to Euler's totient function $\phi(N)$,and a private exponent d connected via the relation $ed = 1 \bmod N$. The following algorithms describe the initial schemes of the RSA cryptosystem in details.

Algorithm 1: RSA Key Generation
Input: The bitsize n of the modulus **Output:** A public key $(N;\ e)$ and a private key $(N;\ d)$

[22] May, A. (2003). New RSA vulnerabilities using lattice reduction methods (Doctoral dissertation, University of Paderborn).

[23] Hoffstein, J., Pipher, J., Silverman, J. H., Silverman, J. H. (2008). An introduction to mathematical cryptography (Vol. 1). New York: Springer.

[24] Rivest, R., Shamir, A., Adleman, L. (1978). A Method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, vol. 21, pp. 120-126.

1. Generate two large random and distinct primes p and q with ($n =$ 2)-bit primes size

2. Compute the modulus $N = pq$ and $\phi(N) = (p-1)(q-1)$.

3. Choose a random integer e satisfying gcd $(e; \phi(N)) = 1$

4. Compute an integer d such that $d \equiv e^{-1} mod\ \phi(N)$.

5. Return the public key $(N; e)$ and the private key $(N; d)$

Algorithm 2: RSA Encryption

Input: The public key $(N; e)$ and the original message M

Output: The ciphertext C

1. Choose a message $M \in Z_N^+$

2. Compute the $C \equiv M^e \ (mod\ N)$

3. Return the ciphertext C

Algorithm 3: RSA Decryption

Input: The private key $(N; d)$ and the ciphertext C

Output: The original message M

1. Compute the $M \equiv C^d \ (mod\ N)$

2. Return the message M

From Algorithm 2 and 3, it can be seen that both parameters e and d will be used respectively, as public and private exponents modulo the large RSA modulus, which is, in general, deemed as computationally costly. Over the years, variants of RSA have been designed in order to increase efficiency

and to reduce cost of implementation. Works by Rabin et al.[25] are the instances of variants of RSA. An interested reader may refer to *Hinek, M. J. Cryptanalysis of RSA and its variants* for further explanation. Another popular method to reduce the cost of the decryption and the signature generation is to use a short private exponent d. It is related to the public exponent e by the above congruence relations vis-`a-vis the equation $ed - k\phi(N) = 1$. Unfortunately, this might render RSA insecure.

Indeed, in 1990, Wiener's work[26] indicated that the RSA modulus N can be factored if $d < \frac{1}{3}N^{0.25}$ by the continued fraction attack. Using Coppersmith's technique and lattice reduction, Boneh et al.[27] enhanced the attack range up to$d < N^{0.292}$. Later on, Blomer et al. improved Wiener's work, and presented a generalized equation in the form $ex + y = k\phi(N)$. They utilized the continued fraction method and Coppersmith's technique and exposed that the solution for $ex + y = k\phi(N)$ can be obtained if $x < \frac{1}{3}N^{0.25}$ and $|y| < N^{-0.75}ex$. Note that the bound of Boneh et al. is valid essentially when e is of the same magnitude than N. [13] extended the

---

[25] Quisquater, J.-J., Couvreur, C. (1982): Fast decipherment algorithm for RSA public key cryptosystem. Electronics Letters, vol. 18(21), pp. 905-907.

Rabin, M. O. (1979). Digitalized signatures and public-key functions as intractable as factorization. Massachusetts Inst of Tech Cambridge Lab for Computer Science.

Takagi, T. (2004). A fast RSA-type public-key primitive modulo p k q using Hensel lifting. IEICE transactions on fundamentals of electronics, communications and computer sciences, 87(1), 94-101.

[26] Wiener, M. (1990). Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, vol.36, pp. 553-558.

[27] Boneh, D., Durfee, G. (1999). Cryptanalysis of RSA with private key d less than $N^{0:292}$. In: LNCS of Advances in Cryptology-EUROCRYPT'99, vol. 12, pp. 1-13.

attack of Boneh et al. with the equation $ed - k\phi(N)$=1 for arbitrary $e < N^{\beta}$ and $d < N^{\delta}$. They showed that RSA is vulnerable if $\delta < 1 - \frac{1}{2}\sqrt{2\beta}$ .In 2018, Bunder and Tonien proposed an attack on the RSA utilising continued fraction expansion over $\frac{e}{N'}$ where N' is a value that depends on the modulus N. They proved that the RSA is susceptible when $d < 2\sqrt{2}N^{\frac{3}{4}-\frac{t}{2}}$.

Another attack on the small decryption exponent was proposed by Weger[28] using the primes difference method. He proved that the RSA is insecure when $d < \frac{N^{\frac{3}{4}}}{|p-q|}$. In 2012, Nitaj[29] also proposed an attack on the RSA using the same method and he managed to improved Wiener's bound up to $\frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$. Later in 2018, Ariffin et al. generalized Nitaj's work and described an attack on the RSA using a combination of the small prime and continued fractions expansion methods and showed that when $d < \frac{\sqrt{3}}{\sqrt{2}}N^{\frac{3}{4}-\gamma}$, one can find d and k which then can lead to the factorization of the modulus N.

Note that if d satisfies the equation $ed - k\phi(N) = 1$ then the continued fraction expansion of $\frac{e}{\varphi(N)}$ would yield the candidates for $\frac{k}{d}$ in the list of the convergents. Exploiting this fact, from the relation $ea - \phi(N)b = c$ with $0 < a < d, 0 < b < k$ and is suitably small, if one obtains the convergent

---

[28] Wiener, M. (1990). Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, vol.36, pp. 553-558.

[29] Nitaj, A. (2009). Cryptanalysis of RSA using the ratio of the primes. In International Conference on Cryptology in Africa (pp. 98-115). Springer, Berlin, Heidelberg.

of $\frac{a}{b}$ which corresponds to $\frac{e}{\varphi(N)}$, the factorization of the RSA modulus $N = pq$ is feasible. In this work, we study the RSA's public parameter associated with the equation of the form

$ea - \phi(N)b = c$ with

$e = N^{\beta}$, $0 < a < N^{\delta}$, $0 < |c| < N^{\gamma}$

Using Coppersmith's method and lattice reduction techniques, we show that if

$\delta < 1 - \frac{1}{2}\gamma - \frac{1}{2}\sqrt{2\beta}$, $\beta > \frac{1}{2}$,

then the modulus N can be factored.

If $\gamma = 0$, we get $\delta < 1 - \frac{1}{2}\sqrt{2\beta}$ which retrieves the u_i bounds of Kamel Ariffin[30], Kumar et al., Bunder et al.[31], for the equation $ed - k\phi(N) = 1$. Moreover, if $\beta = 1$, we get $\delta < 1 - \frac{1}{2}\sqrt{2} \approx 0.292$, which retrieves the bound of Boneh et al. As a consequence, our new attack fully covers both attacks of Boneh et al., and Kumar et al. on RSA. The method presented in this work shows that the set of the weak public exponents e in the attacks of Boneh et al., and Kumar et al. can be expanded to more exponents.

The initiation for the new attack is the equation $ea - \phi(N)b = c$.

In all cases, we transform it to two a modular polynomial equation $f(y_1; y_2; y_3) \equiv 0 (mod\ e)$ with $f(y_1; y_2; y_3) = y_1 y_2 + a_1 y_2 + y_3$ and

---

[30] Kamel Ariffin, M. R., Abubakar, S. I., Yunos, F., & Asbullah, M. A. (2019). New crypt- analytic attack on RSA modulus N= pq using small prime di_erence method. Cryptography, 3(1),

[31] Bunder, M. W., & Tonien, J. (2017). A new attack on the RSA cryptosystem based on continued fractions. Malaysian Journal of Mathematical Sciences, vol. 11(S), pp. 45-57.

$f(y_1, u) \equiv 0(mod\ e)$ with $F(y_1;\ u) = u\ +\ a_1 y_3$ and $u = y_1 y_2 + y_3$ .To find the small solutions of the modular equation $f(y_1; y_2; y_3) \equiv\ 0(mod\ e)$, we use Coppersmith's technique[32], and lattice reduction, combines with the strategies presented in Herrmann and May[33] as well as in Jochemsz[34]. Under the condition that the parameters a and c are suitably small, the solutions of the modular equation lead to the factorization of the RSA modulus.

This work has been divided into the following sections. The first reviews on lattice reduction and Coppersmith's technique. The second section describes the new attack on RSA while the third section presents a comparison of the new attack with the existing attacks. Lastly provides the conclusion for this study.

5.2 Preliminaries

This section briey present basics yet important materials on lattice reduction and Coppersmith's technique.

---

[32] Coppersmith, D. (1997). Small solutions to polynomial equations, and low exponent RSA vulnerabilities. In: LNCS of Advances in Cryptology-EUROCRYPT'99, vol. 10, pp.233-260.

[33] Herrmann, M., & May, A. (2010, May). Maximizing small root bounds by linearization and applications to small secret exponent RSA. In *International Workshop on Public Key Cryptography* (pp. 53-69). Springer, Berlin, Heidelberg.

[34] Jochemsz, E., & May, A. (2006, December). A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 267-282). Springer, Berlin, Heidelberg.

5.2.1 Lattice Reduction

Let $u_1, \ldots, u_\omega$ be ω linearly independent vectors of R^n with $\omega \leq n$. The lattice $\mathcal{L}$ spanned by $(u_1, \ldots, u_\omega)$ is the set of all integer linear combinations of the u_i.

Namely,

$$\mathcal{L} = \sum_{i=1}^{\omega} x_i \, u_i | x_i | \in \mathbb{Z}$$

Let U be the basis matrix, that is the matrix of the set $(u_1, \ldots, u_\omega)$ in the canonical basis of R^n. The determinant of $\mathcal{L}$ is defined as $det(\mathcal{L}) = \sqrt{\det(U^t U)}$. The determinant reduces to $det(\mathcal{L}) = |\det(U)|$ when $\omega = n$. The set $(u_1, \ldots, u_\omega)$ is called a basis of $\mathcal{L}$ with dimension ω. Denote by $\|v\|$ the Euclidean norm of a vector $v \in \mathcal{L}$. The main problem in lattice reduction is to find short non-zero vectors in $\mathcal{L}$. It is known that vectors with enough short norms can be found with the aid of using LLL algorithm[35].

Theorem 6.1. *Suppose that the lattice spanned by a basis* $u_1, \ldots, u_\omega$ *denoted by* $\mathcal{L}$. *Then a new basis* $(b_1, \ldots, b_\omega)$ *of* $\mathcal{L}$ *will be produced by LLL algorithm satisfies:*

$$\|b_1\| \leq \ldots \leq \|b_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}}$$

for $i = 1,2,\ldots,\omega$.

---

[35] Lenstra, A.K., Lenstra,H.W., Lov_asz, L. (1982). Factoring Polynomials with rational coefficients. Mathematische Annalen, vol. 261, pp. 513-534.

The complexity of the LLL algorithm depends on the dimension ω and on the maximum bitsize of the entries of the lattice matrix.

5.2.2 Coppersmith's method

In Coppersmith's work, new techniques to find small modular roots of polynomials in one variable, and solutions of polynomial equations in two variables over the integers was presented. For better understanding, one may refer to Galbraith's work[36]. Since its invention, the ideas of Coppersmith have been heuristically extended to more than two variables. This was possible by applying a theorem in Howgrave-Graham's work[37]. For example, for a polynomial $h(y_1, y_2, y_3, u) = \sum_{i_1,i_2,i_3,i_4} a_{i,j,k} y_1^{i_1} y_2^{i_2} y_3^{i_3} u^{i_4}$ with the Euclidean norm $h(y_1, y_2, y_3, u) = \sqrt{\sum_{i_1,i_2,i_3,i_4} a_{i,j,k}^2}$ Howgrave-Graham's theorem reduces to the following result.

Theorem 6.2. *Let* $h(y_1, y_2, y_3, u) \in \mathbb{Z}[y_1, y_2, y_3, u]$ *be a polynomial with at most* ω *monomials. Suppose* $h\left(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}\right) \equiv 0 \ (mod\ e^m)$, *provided that* $h(y_1, y_2, y_3, u) < e^{\frac{m}{\sqrt{\omega}}}$, *where* $\left|y_1^{(0)}\right| < Y_1$, $\left|y_2^{(0)}\right| < Y_2$, $\left|y_3^{(0)}\right| < Y_3$ *and* $\left|u^{(0)}\right| < U$. *Then* $h\left(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}\right) = 0$ *holds over integers.*

To find the roots of a system of polynomials, we use the Gröbner basis technique. As required by most multivariate applications of Coppersmith's technique, finding the roots relies on the subsequent assumption.

---

[36] Galbraith, S. D. (2012). Mathematics of public key cryptography. Cambridge University Press.

[37] Howgrave-Graham, N. (1997). Finding small roots of univariate modular equations revisited. In: LNCS of Cryptography and Coding, pp. 131-142.

Assumption 6.1. *Let* $h(y_1, y_2, y_3, u) \in \mathbb{Z}[y_1, y_2, y_3, u]$ *be the polynomial that are found by LLL algorithm. Then the ideal generated by the polynomial equation* $h_1(y_1, y_2, y_3, u) = 0$, $h_2(y_1, y_2, y_3, u) = 0$, $h_3(y_1, y_2, y_3, u) = 0$, $h_4(y_1, y_2, y_3, u) = 0$ *has dimension zero.*

Note that in our attack, the strategy of Jochemsz-May[38] that we utilised implemented the Coppersmith's method in order to find the roots of a polynomial. They reformulated the idea from Coron's work[39], and came out with a strategy to find the roots of either modular or integer multivariate polynomial.

5.3 The Proposed Attack on RSA

A new attack on RSA will be described throughout this section. We examine the case where the RSA public parameters $(N; e)$ satisfies an equation $ea - \phi(N) = c$ where $\phi(N) = (p-1)(q-1)$ and a and $|c|$ are suitably small unknown integers.

---

[38] Jochemsz, E., May, A. (2006). A strategy for _nding roots of multivariate polynomials with new applications in attacking RSA variants. In: LNCS of Advances in Cryptology- ASIACRYPT 2006, pp. 267-282.

[39] Coron, J. S. (2004, May). Finding small roots of bivariate integer polynomial equations revisited. In International Conference on the Theory and Applications of Cryptographic Techniques Springer, Berlin, Heidelberg. pp. 492-505.

Theorem 6.3. *Let the modulus and the public exponent of the RSA be* $N = pq$ *and* $e = N^{\beta}$ *respectively with* $\beta > \frac{1}{2}$ *. Suppose that satisfies the equation* $ea - (p-1)(q-1)b = c$ *with* $a < N^{\delta}$ *and* $|c| < N^{\gamma}$ *. If* $\delta < 1 - \frac{1}{2}\gamma - \frac{1}{2}\sqrt{2\beta} - \varepsilon$ *, then following the Assumption 6.1, the modulus can be factored in polynomial time.*

Proof. Let $N = pq$ be an RSA modulus, e be its public exponent and e is required to satisfy $ea - (p-1)(q-1)b = c$. Then $-b(N + 1 - p - q) - c \equiv 0 \ (mod\ e)$. Expanding this equation, we have $b(p+q) - (N+1)b - c \equiv 0 \ (mod\ e)$. Consider the polynomial

$$f(y_1, y_2, y_3) = y_1 y_2 + a_1 y_1 + y_3$$

where $a_1 = -(N+1)$. Then the polynomial modular equation $f(y_1, y_2, y_3) \equiv 0 \ (mod\ e)$ would yield $\left(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}\right) = (b, p+q, -c)$ as its solution. To obtain the intended roots of this modular equation Coppersmith's method combined with Jochemsz and May's strategy for choosing the extra shifts.

Let $s, t \in \mathbb{Z}^+$ that will be determined next. For $0 \le r \le s$, assign the set $M_r = \bigcup_{0 \le j \le t} \{ y_1^{i_1} y_2^{i_2+j} y_3^{i_3} \mid y_1^{i_1} y_2^{i_2} y_3^{i_3}$ is a monomial of $f^s(y_1, y_2, y_3)$ and $\frac{y_1^{i_1} y_2^{i_2} y_3^{i_3}}{(y_1 y_2)^r}$ is a monomial of $f^{s-r}\}$.

A direct computation shows that $f^s(y_1, y_2, y_3)$ is

$$f^s(y_1, y_2, y_3) = \sum_{i_1=0}^{s} \sum_{i_2=0}^{i_1} \binom{s}{i_1} \binom{i_1}{i_2} a_1^{i_1 - i_2} \ y_1^{i_1} y_2^{i_2} y_3^{s-i_1}$$

Hence $y_1^{i_1} y_2^{i_2} y_3^{i_3}$ is a monomial of $f^s(y_1, y_2, y_3)$ if

$$i_1 = 0, \ldots, s \ ; \ i_2 = 0, \ldots, i_1 \ ; \ i_3 = s - i_1$$

Similarly, $y_1^{i_1}y_2^{i_2}y_3^{i_3}$ is a monomial of $f^{s-r}(y_1,y_2,y_3)$ if

$$i_1 = 0,\dots,s-r\ ;\ i_2 = 0,\dots,i_1\ ;\ i_3 = s-r-i_1$$

Hence, for $0 \le r \le s$, if $y_1^{i_1}y_2^{i_2}y_3^{i_3}$ is a monomial of $f^s(y_1,y_2,y_3)$ then $\frac{y_1^{i_1}y_2^{i_2}y_3^{i_3}}{(y_1y_2)^r}$ is a monomial of $f^{s-r}(y_1,y_2,y_3)$ if

$$i_1 = r,\dots,s\ ;\ i_2 = r,\dots,i_1\ ;\ i_3 = s-i_1$$

which directs to classification of the set M_r . For $0 \le r \le s$, we have

$y_1^{i_1}y_2^{i_2}y_3^{i_3} \in M_r$ if $i_1 = r,\dots,s\ ;\ i_2 = r,\dots,i_1+t\ ;\ i_3 = s-i_1$.

Substitute r by $r\ +\ 1$, we obtain

$y_1^{i_1}y_2^{i_2}y_3^{i_3} \in M_{r+1}$ if $i_1 = r+1,\dots,s\ ;\ i_2 = r+1,\dots,i_1+t;\ i_3 = s-i_1$

For $0 \le r \le s$, define the following polynomials

$g_{r,i_1,i_2,i_3}(y_1,y_2,y_3) = \frac{y_1^{i_1}y_2^{i_2}y_3^{i_3}}{(y_1y_2)^r}f(y_1,y_2,y_3)^r e^{s-r}$ with $y_1^{i_1}y_2^{i_2}y_3^{i_3} \in M_r \setminus M_{(r+1)}$

Since

$$y_1^{i_1}y_2^{i_2}y_3^{i_3} \in M_r \setminus M_{r+1}$$

$$\text{if } i_1 = r,\dots,s\ ;\ i_2 = r\ ;\ i_3 = s-i_1$$

$$\text{or } i_1 = r\ ;\ i_2 = r+1,\dots,i_1+t\ \ ;\ i_3 = s-i_1$$

then the polynomials $g_{r,i_1,i_2,i_3}(y_1,y_2,y_3)$ reduce to the polynomials $A_{r,i_1,i_2,i_3}(y_1,y_2,y_3)$ and $B_{r,i_1,i_2,i_3}(y_1,y_2,y_3)$ where

$A_{r,i_1,i_2,i_3}(y_1,y_2,y_3) = y_1^{i_1-r}y_2^{i_2-r}y_3^{i_3}f(y_1,y_2,y_3)^r e^{s-r}$

$$\text{for } r = 0,\dots,s\ ;\ i_1 = r,\dots,s\ ;\ i_2 = r\ ;\ i_3 = s-i_1$$

$B_{r,i_1,i_2,i_3}(y_1,y_2,y_3) = y_1^{i_1-r}y_2^{i_2-r}y_3^{i_3}f(y_1,y_2,y_3)^r e^{s-r}$

$$\text{for } r = 0,\dots,s\ ;\ i_1 = r\ ;\ i_2 = r+1,\dots,i_1+t\ ;\ i_3 = s-i_1$$

The former polynomials can be slightly transformed as follows

$A_{r,i_1,i_2,i_3}(y_1,y_2,y_3) = y_1^{i_1}y_3^{i_3}f(y_1,y_2,y_3)^r e^{s-r}$

$$\text{for } r = 0,\dots,s\ ;\ i_1 = 0,\dots,s-r\ ;\ i_2 = 0\ ;\ i_3 = s-r-i_1$$

$B_{r,i_1,i_2,i_3}(y_1,y_2,y_3) = y_2^{i_2}y_3^{i_3}f(y_1,y_2,y_3)^r e^{s-r}$

$$\text{for } r = 0,\ldots,s\ ;\ i_1 = 0\ ;\ i_2 = 1,\ldots,t\ ;\ i_3 = s - r$$

Next, we use the linearization technique that has been introduced by Herrmann and May[40]. We transform the polynomial $f(y_1, y_2, y_3) = y_1 y_2 + a_1 y_1 + y_3$ to the reduced polynomial

$$F(y_1, u) = u + a_1 y_1 \qquad u = y_1 y_2 + y_3$$

Using the polynomials $A_{r,i_1,i_2,i_3}(y_1, y_2, y_3)$ and $B_{r,i_1,i_2,i_3}(y_1, y_2, y_3)$ y3), we construct two new families of polynomials where each term $y_1\ and\ y_2$ is replaced by y_3, namely

$$G_{r,i_1,i_2,i_3}(y_1, y_2, y_3, u) = \ y_1^{i_1} y_3^{i_3} F(y_1, u)^r e^{s-r}$$

$$\text{for } r = 0,\ldots,s\ ;\ i_1 = 0,\ldots,s-r\ ;\ i_2 = 0\ ;\ i_3 = s - r\text{-}i_1\ ;\ i_4 = r$$

$$H_{r,i_1,i_2,i_3}(y_1, y_2, y_3, u) = y_2^{i_2} y_3^{i_3} F(y_1, u)^r e^{s-r}$$

$$\text{for } r = \left\lfloor \frac{s}{t} \right\rfloor i_2,\ldots,s\ ;\ i_1 = 0\ ;\ i_2 = 1,..,t\ ;\ i_3 = s - r\ ;\ i_4 = r$$

It follows that the monomials in $G_{r,i_1,i_2,i_3}(y_1, y_2, y_3, u)$ are in the form $y_1^{i_1} y_2^{i_2} y_3^{i_3} u^{i_4}$ with

$$r = 0,\ldots,s\ ;\ i_1 = 0,\ldots,s-r\ ;\ i_2 = 0\ ;\ i_3 = s - r - i_1;\ i_4 = r \tag{5.1}$$

Similarly, the monomials in $H_{r,i_1,i_2,i_3}(y_1, y_2, y_3, u)$ are in the form $y_1^{i_1} y_2^{i_2} y_3^{i_3} u^{i_4}$ with

$$i_1 = 0, i_2 = 1, \ldots t, r = \left\lfloor \frac{s}{t} \right\rfloor i_2,\ldots,s\ ;\ i_1 = 0\ ;\ i_2 = 1,..,t\ ;\ i_3 = s - r\ ;\ i_4 = r \tag{5.2}$$

The lattice denoted as $\mathcal{L}$ is built by the coefficient vectors of the two families of polynomials $G_{r,i_1,i_2,i_3}(y_1 Y_1, y_2 Y_2, y_3 Y_3, uU)$ and $H_{r,i_1,i_2,i_3}(y_1 Y_1, y_2 Y_2, y_3 Y_3, uU)$ where Y_1, Y_2, Y_3, U are integers which will be

---

[40] Herrmann, M., May, A. (2010). Maximizing small root bounds by linearization and applications to small secret exponent RSA. In: LNCS of PKC pp. 53-69.

defined later with the condition $Y_1Y_2y_1y_2 = Uu - Y_3y_3$. The ordering of the rows is such that any polynomial $G_{r,i_1,i_2,i_3}(y_1Y_1, y_2Y_2, y_3Y_3, uU)$ is prior to any polynomial $H_{r,i_1,i_2,i_3}(y_1Y_1, y_2Y_2, y_3Y_3, uU)$, and in $G_{r,i_1,i_2,i_3}(y_1Y_1, y_2Y_2, y_3Y_3, uU)$ or in $H_{r,i_1,i_2,i_3}(y_1Y_1, y_2Y_2, y_3Y_3, uU)$, G_{r,i_1,i_2,i_3} is prior to $G_{r',i_1',i_2',i_3'}$ and H_{r,i_1,i_2,i_3} is prior to $G_{r',i_1',i_2',i_3'}$ is one of the following conditions is satisfied

$r < r'$

$r = r';\ i_1 < i_1'$

$r = r';\ i_1 = i_1';\ i_2 < i_2'$

$r = r';\ i_1 = i_1';\ i_2 = i_2';\ i_3 < i_3'$

$r = r';\ i_1 = i_1';\ i_2 = i_2';\ i_3 = i_3';\ i_4 < i_4'$

A similar rule is applied to order the monomials and the columns. Thus a lower triangular matrix is formed as in the following matrix where $s = 3$ and $t = 2$.

Since the lattice of $\mathcal{L}$ is a lower triangular matrix, thus the determinant is obtained by multiplying the diagonal terms. Since only Y_1, Y_2, Y_3, U and e are involved, then determinant is of the form

$$\det(\mathcal{L}) = Y_1^{nY_1}Y_2^{nY_2}Y_3^{nY_3}U^{nU}e^{n_e} \tag{5.3}$$

Using the construction of the monomials of the polynomials $G_{r,i_1,i_2,i_3,i_4}(y_1, y_2, y_3, u)$ and $H_{r,i_1,i_2,i_3,i_4}(y_1, y_2, y_3, u)$ where r, i_1, i_2, i_3, i_4 satisfy the conditions (6.1) and (6.2), the dominant terms of the exponents $nY_1, nY_2, nY_3, nU, n_e$ as well as the dimension ω of the lattice satisfy

$$nY_1 = \sum_{r=0}^{s}\sum_{i_1=0}^{s-r} i_1 = \frac{1}{6}s^3 + o(s^3)$$

$$nY_2 = \sum_{i_2=1}^{t}\sum_{r=\left\lfloor\frac{s}{t}\right\rfloor}^{s} i_2 = \frac{1}{2}st^2 - \frac{1}{3}\left\lfloor\frac{s}{t}\right\rfloor t^3 + o(s^3)$$

$$nY_3 = \sum_{r=0}^{s}\sum_{i_1=0}^{s-r}(s-r-i_1) + \sum_{i_2=1}^{t}\sum_{r=\lfloor\frac{s}{t}\rfloor}^{s}(s-r)$$
$$= \frac{1}{6}s^3 + \frac{1}{2}st^2 - \frac{1}{2}\left\lfloor\frac{s}{t}\right\rfloor s^2t + \frac{1}{6}\left\lfloor\frac{s}{t}\right\rfloor^2 t^3$$
$$nU = \sum_{r=0}^{s}\sum_{i_1=0}^{s-r} r + \sum_{i_2=1}^{t}\sum_{r=\lfloor\frac{s}{t}\rfloor}^{s} r$$
$$= \frac{1}{6}s^3 + \frac{1}{2}st^2 + \frac{1}{6}\left\lfloor\frac{s}{t}\right\rfloor^2 t^3$$
$$n_e = \sum_{r=0}^{s}\sum_{i_1=0}^{s-r}(s-r) + \sum_{i_2=1}^{t}\sum_{r=\lfloor\frac{s}{t}\rfloor}^{s}(s-r)$$
$$= \frac{1}{3}s^3 + \frac{1}{2}s^2t + \frac{1}{6}\left\lfloor\frac{s}{t}\right\rfloor^2 t^3 - \frac{1}{2}\left\lfloor\frac{s}{t}\right\rfloor st^2$$
$$\omega = \sum_{r=0}^{s}\sum_{i_1=0}^{s-r} 1 + \sum_{i_2=1}^{t}\sum_{r=\lfloor\frac{s}{t}\rfloor}^{s} 1 = \frac{1}{2}s^2 + st - \frac{1}{2}\left\lfloor\frac{s}{t}\right\rfloor t^2$$

In the following asymptotic analysis, we set $t = rs$ with $0 < r \leq 1$ and use $\left\lfloor\frac{s}{t}\right\rfloor \approx 1/r$. Then, for sufficiently large s, the exponents $nY_1, nY_2, nY_3, nU, n_e$ and the dimension ω reduce to

$$nY_1 = \frac{1}{6}s^3 + o(s^3)$$
$$nY_2 = \frac{1}{6}r^2s^3 + o(s^3)$$
$$nY_3 = \tfrac{1}{6}(r+1)s^3 + o(s^3)$$
$$nU = \frac{1}{6}(2r+1)s^3 + o(s^3)$$
$$n_e = \frac{1}{6}(r+2)s^3 + o(s^3)$$
$$\omega = \frac{1}{2}(r+1)s^3 + o(s^3)$$

(5.4)

To apply Theorem 6.1 with $i = 4$ to the four shortest vectors in the LLL-reduced basis of $\mathcal{L}$, we set

$$2^{\frac{\omega(\omega-1)}{4(\omega-3)}} \det(\mathcal{L})^{\frac{1}{\omega-3}} < \frac{e^s}{\sqrt{\omega}}$$

This transform to

$$\det(\mathcal{L}) < \frac{2^{-\frac{\omega(\omega-1)}{4}}}{(\sqrt{\omega})^{\omega-3}} e^{s(\omega-3)}$$

Then, using (6.3), we get

$$e^{n_e - s\omega} Y_1^{nY_1} Y_2^{nY_2} Y_3^{nY_3} U^{nU} < \frac{2^{-\frac{\omega(\omega-1)}{4}}}{(\sqrt{\omega})^{\omega-3}} e^{s(\omega-3)} \tag{5.5}$$

Suppose that from $ea - (p-1)(q-1)b = c$ we have $e = N^{\beta}$, $a < N^{\delta}$ and $|c| < N^r$. We set

$$Y_1 = 2N^{\beta+\delta-1},\ Y_2 = 3N^{\frac{1}{2}},\ Y_3 = N^r,\ U = 12N^{\beta+\delta-\frac{1}{2}} \tag{5.6}$$

Then the target solution $\left(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}\right) = (b, p+q, -c, b(p+q) + a_1 b)$ satisfies $\left|y_2^{(0)}\right| < p+q < Y_2$, $\left|y_3^{(0)}\right| = |c| < Y_3$; and

$$\left|y_1^{(0)}\right| = b = \frac{(ea-c)}{\phi(N)} < \frac{ea+|c|}{\phi(N)} < 2N^{\beta+\delta-1} \tag{5.7}$$

where we used $\phi(N) \approx N$. Hence, $\left|y_1^{(0)}\right| < Y_1$. It follows that

$$\begin{aligned} \left|u^{(0)}\right| = \left|y_1^{(0)} y_2^{(0)} + y_3^{(0)}\right| &< 2\max(Y_1 Y_2 + Y_3) \\ &= 2\max\left(2N^{\beta+\delta-1} 3N^{\frac{1}{2}} + N^r\right) \\ &= 12N^{\beta+\delta-\frac{1}{2}} \end{aligned}$$

and consequently $\left|u^{(0)}\right| < U$. Using the values $nY_1, nY_2, nY_3, nU, n_e$ and ω from (6.4) as well as the values of Y_1, Y_2, Y_3 and U from (6.6), we get

$e^{n_e - s\omega} = N^{\left(-\frac{1}{3}r - \frac{1}{6}\right)\beta s^3 + o(s^3)}$

$Y_1^{nY_1} = 2^{\frac{1}{6}s^3 + o(s^3)} N^{\frac{1}{6}(\beta+\delta-1)s^3 + o(s^3)} = N^{\frac{1}{6}(\beta+\delta-1)s^3 + o(s^3) + \varepsilon_1}$

$$Y_2^{nY_2} = 3^{\frac{1}{6}r^2s^3+o(s^3)}N^{\frac{1}{2}r^2s^3+o(s^3)} = N^{\frac{1}{2}r^2s^3+o(s^3)+\varepsilon_2}$$

$$Y_3^{nY_3} = N^{(\frac{1}{6}r+\frac{1}{6})\gamma s^3+o(s^3)}$$

$$U^{nU} = 12^{(\frac{1}{3}r+\frac{1}{6})s^3+o(s^3)}N^{\left(\frac{1}{3}r+\frac{1}{6}\right)(\beta+\delta-1)s^3+o(s^3)} = N^{\left(\frac{1}{3}r+\frac{1}{6}\right)(\beta+\delta-1)s^3+o(s^3)+\varepsilon_3}$$

$$\frac{2^{-\frac{\omega(\omega-1)}{4}}}{(\sqrt{\omega})^{\omega-3}}e^{-3s} = N^{-2\beta-\varepsilon_4}$$

where $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4 \in \mathbb{Z}^+$ and their values are small depending on s and N. Then, taking logarithms, dividing by $s3\,logN$ and letting $\varepsilon_5 > 0$ for the contributions of the small terms, the inequality (6.5) leads to

$$\left(-\frac{1}{3}r-\frac{1}{6}\right)\beta+\frac{1}{6}(\beta+\delta-1)+\frac{1}{12}r^2+\left(\frac{1}{6}r+\frac{1}{6}\right)\gamma+\left(\frac{1}{3}r+\frac{1}{6}\right)\left(\beta+\delta-\frac{1}{2}\right)<\varepsilon_5$$

where $\varepsilon_5 \in \mathbb{Z}^+$ is a small value and depends on s and N. Then, rearranging, we get

$$r^2+(4\delta+2\gamma-2)r+2\beta+4\delta+2\gamma-3<-12\varepsilon_5 \tag{5.8}$$

From the left side of (6.8), the value for γ is optimum when

$$r_0 = 1-2\delta-\gamma$$

Here we need $r_0 > 0$. This is achieved if

$$\delta < \frac{1}{2}-\frac{1}{2}\gamma \tag{5.9}$$

Replacing r_0 in (6.8), we get

$$-4\delta^2+(8-4\gamma)\delta+4\gamma+2\beta-\gamma^2-4<12\varepsilon_5$$

which will be true if

$$\delta < 1-\frac{1}{2}\gamma-\frac{1}{2}\sqrt{2\beta}-\varepsilon \tag{5.10}$$

where $\varepsilon\epsilon\mathbb{Z}^+$ is a small value and depends on s and N. Since δ satisfies (6.9) and (6.10) and $\beta > \frac{1}{2}$ then

$$\delta < min\left(1-\frac{1}{2}\gamma-\frac{1}{2}\sqrt{2\beta}-\varepsilon, \frac{1}{2}-\frac{1}{2}\gamma\right) = 1-\frac{1}{2}\gamma-\frac{1}{2}\sqrt{2\beta}-\varepsilon$$

Using the first four vectors $u_1, u_2, u_3\, u_4$ in the LLL reduced basis, we get four vectors $g_1(y_1, y_2, y_3, u)$, $g_2(y_1, y_2, y_3, u)$, $g_3(y_1, y_2, y_3, u)$, $g_4(y_1, y_2, y_3, u)$ such that

$$g_1\left(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}\right) = g_2\left(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}\right) = g_3\left(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}\right) = g_4\left(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}\right) = 0$$

Assume that $g_1(y_1, y_2, y_3, u)$, $g_2(y_1, y_2, y_3, u)$, $g_3(y_1, y_2, y_3, u)$, $g_4(y_1, y_2, y_3, u)$ are algebraically independent, we apply resultant techniques or Grobner basis method to find the solution $\left(y_1^{(0)}, y_2^{(0)}, y_3^{(0)}, u^{(0)}\right) = (b, p+q, -c, b(p+q) + a_1 b)$. From $y_2^{(0)} = p + q$ and $N = pq$, we get p and q. Thus, this gives the factorization of N.

5.4 Comparison with Existing Results

5.4.1 Comparison with the result in Boneh-Durfee's work.

For the balanced primes p and q and in the presence of an encryption exponent e of the same magnitude to N, Boneh and Durfee showed that the RSA modulus $N = pq$ is factorable satisfying its original key equation $ed - k\phi(N) = 1$ with

$\delta < 1 - \frac{\sqrt{2}}{2} \approx 0.292$ for $d < N^{\delta}$

In the equation $ea - \phi(N)b = c$ with $e = N^{\beta}$, $a < N^{\delta}$, and $|c| < N^{\gamma}$, this corresponds to $\beta = 1$ and $\gamma = 0$. Plugging these values in $\delta < 1 - \frac{1}{2}\gamma$, we get

$\delta < 1 - \frac{\sqrt{2}}{2} \approx 0.292$

which recovers the same bound as in Boneh-Durfee's work. Observe that when $a = d$, $b = k$, $c = 1$, then the original RSA key equation is a particular case of the equation $ea - \phi(N)b = c$. This implies that the class

of the weak exponents in Boneh-Durfee's work is a subclass of the weak exponents of the new attack.

5.4.2 Comparison with the result in Kumar-et al.'s work

The result presented in Kumar-et al.'s work extended the attack of Boneh and Durfee's work to all exponents $e = N^{\beta}$ and demonstrate that N can be factored with

$$\delta < 1 - \frac{1}{2}\sqrt{2}\beta \qquad \text{where } d < N^{\delta}$$

Note that $ed - k\phi(N) = 1$ is a particular equation of $ea - \phi(N)b = c$ whenever $c = N^{\gamma} = 1$ that is $\gamma = 0$. Plugging this value in the new bound $\delta < 1 - \frac{1}{2}\gamma - \frac{1}{2}\sqrt{2\beta} - \varepsilon$, we get

$$\delta < 1 - \frac{1}{2}\sqrt{2\beta} - \varepsilon$$

which retrieves the bound of Kumar et al.'s work. Moreover, as in the previous comparison, the class of the weak exponents in this work is a subclass of the weak exponents of the new attack.

5.4.3 Comparison with the result in Blomer-May's work.

A cryptanalysis result on RSA presented in Blomer-May's work show that for encryption exponent satisfies an equation $ex - y\phi(N) = z$ with $0 < |x| \leq \frac{1}{3}\sqrt{\frac{\phi(N)}{e}}\frac{N^{\frac{3}{4}}}{p-q}$ an$|z| \leq \frac{p-q}{\phi(N)N^{\frac{1}{4}}}ex$, then the RSA modulus can be factored. Suppose that $|x| < N^{\delta}$, $e = N^{\beta}$ and $p - q = cN^{\frac{1}{2}}$ for some constant $c < 1$. Then, the attack in this work can be applied only if

$\delta < \frac{3}{4} - \frac{1}{2}\beta$ and $\gamma < \beta + \delta - \frac{3}{4}$

Hence, in the situation $e \approx N^{\beta}$, that is $\beta = 1$, therefore such attack is applicable only for $\delta < \frac{1}{4}$ and $\gamma < \frac{1}{2}$ while our attack is applicable whenever the conditions of Theorem 6.3 are satisfied with $\beta = 1$, that is whenever

$$\delta < 1 - \frac{1}{2}\gamma - \frac{1}{2}\sqrt{2} - \varepsilon \approx 0.292 - \frac{1}{2}\gamma$$

This is better than the bound in Blomer-May's work when $0.292 - \frac{1}{2}\gamma > \frac{1}{4}$, that is for $\gamma < 0.048$.

5.4.4 Comparison with the result in Bunder-Tonien's work.

Bunder and Tonien described an attack on the RSA by using the continued fraction expansion. However, instead of finding the convergents of $\frac{e}{N}$, they find the convergents of $\frac{e}{N'}$ where N' is given by $N' = \left[N - \left(a + \frac{3}{2\sqrt{2}}\right)N^{\frac{1}{2}} + 1\right]$. In their attack, they showed that for $e \approx N^{\beta}$, they can recover the private exponent when

$$d < 2\sqrt{2}N^{\frac{3}{4}-\frac{\beta}{2}}$$

Note that the authors also used the original key equation, $ed - k\phi(N) = 1$. Thus, in comparison, we let $c = N^{\gamma} = 1$ which indicates that $\gamma = 0$. Thus we have

$$\delta < 1 - \frac{1}{2}\sqrt{2\beta} - \varepsilon$$

In order to find $\max\{\frac{3}{4} - \frac{\beta}{2}, 1 - \frac{1}{2}\sqrt{2\beta} - \varepsilon\}$, we first assume that the bound of Bunder-Tonien's work is bigger than our bound. Neglecting the coefficients, we get

$$\frac{3}{4} - \frac{\beta}{2} - \left(1 - \frac{1}{2}\sqrt{2\beta} - \varepsilon\right) > 0$$

$$-\frac{1}{4}-\frac{\beta+\sqrt{2\beta}}{2}>0 \qquad (5.11)$$

Since we know that $0<\beta\leq 1$, to illustrate we randomly choose any two values within that bound and substitute them into (6.11). As an example, we obtain $-\frac{7+2\sqrt{10}}{20}$ and $-\frac{-3+2\sqrt{2}}{4}$ for $\beta=0.2$ and $\beta=1$ respectively. These values contradict to inequality in (6.11) which shows that our bound is greater than Bunder and Tonien's work. Thus, we improve their bound.

5.4.5 Comparison with the result in Ariffin-et al.'s work.

Ariffin et al. proposed a short decryption exponent attack on the RSA. Using the small prime difference method of the form $|b^2p-a^2q|<N^\gamma$ where the ratio of $\frac{b^2}{a^2}$ is approximately close to $\frac{p}{q}$, they show that one can find $\frac{k}{d}$ from the convergents of the continued fraction expansion of $\frac{e}{N-\left\lfloor\frac{a^2b^2}{ab}\sqrt{N}\right\rfloor+1}$ whenever

$$d<\frac{\sqrt{3}}{\sqrt{2}}N^{\frac{3}{4}\gamma} \quad \text{for} \quad |b^2p-a^2q|<N^\gamma \qquad (5.12)$$

Since Ariffin et al. used the key equation $ed-k\phi(N)=1$, thus for our bound, we let $\gamma=0$. Thus we have

$$\delta<1-\frac{1}{2}\sqrt{2\beta}-\varepsilon$$

From (6.12), it can be seen that their bound only depends on and they have stated that $0.25\leq\gamma<0.5$. Meanwhile, our bound depends on the size of β such that $\beta=\log_N e$. We present the comparison of bound in the following tables.

Table 2: Comparison with methoda from Ariffin et al. for $\gamma = 0{,}25$.

Bound of δ \ $\beta = \log_N(e)$	$\beta = 1$	$\beta = 0.8$	$\beta = 0.6$	$\beta = 0.4$	$\beta = 0.2$
Ariffin et al.	0.50	0.50	0.50	0.50	0.50
Our bound	0.29	0.36	0.45	0.55	0.68

Table 3: Comparison with methoda from Ariffin et al. for γ=0,45.

Bound of δ \ $\beta = \log_N(e)$	$\beta = 1$	$\beta = 0.8$	$\beta = 0.6$	$\beta = 0.4$	$\beta = 0.2$
Ariffin et al.	0.30	0.30	0.30	0.30	0.30
Our bound	0.29	0.36	0.45	0.55	0.68

The tables above show that our bound is increasing as the value of β is decreasing. From Table 2, we manage to improve Ariffin et al.'s work when $\beta = 0.4$ and from Table 3, we improve Ariffin-et al.'s work when $\beta = 0.8$. This indicates that our bound is better Ariffin et al.'s work for smaller values of β.

5.4.6 A numerical example

As a numerical example, let us consider the RSA public key (N, e) with

N
$= 5339583385665627056733057342119365266735235221280290598464283$
e
$= 387352723307775993183504910232949247618286415301692228843681$

Observe that for e and N satisfy an equation $ea - (p-1)(q-1)b = c$. Define the polynomial $f(y_1, y_2, y_3) = y_1 y_2 + a_1 y_1 + y_3$ where $a_1 = -(N +$

1), $y_1 = b,\ y_2 = p + q,\ y_3 = -c$. Then, applying the method of Theorem 6.3 with the parameters

$$s = 5, t = 3, Y_1 = 2\left\lfloor N^{\frac{1}{4}} \right\rfloor, Y_2 = 3\left\lfloor N^{\frac{1}{2}} \right\rfloor, Y_3 = \lfloor N^{0.06} \rfloor, U = 12N^{0.74}$$

We get a lattice dimension of Executing the LLL algorithm followed by the resultant technique, we obtain small solutions from systems of polynomial equations as follows;

$y_1 = 660305687366885$
$y_2 = 462232197246100674972501649396$
$y_3 = -4183$
$u = 3052145487256920739455170538527222831651718277$

Hence, $p + q = y_2 = 462232197246100674972501649396$, which is sufficient to compute its corresponding prime factors

$$p = 235453976685336037060153059493 7$$
$$q = 226778220560764637912348589905 9$$

We notice that, using $\phi(N) = (p-1)(q-1)$, we get

$d \equiv e^{-1}(mod(N))$
$\equiv 592294212514666735434888502687363310152982843784672392529585$

Hence,$d \approx N^{0.981} \gg N^{0.292}$. This is clearly an exponential increment of the RSA attack range. This shows that the attacks of Boneh-Durfee, Kumar et al., Ariffin et al. and Bunder-Tonien can not be applied for the key (e, N). We also are able to retrieve the values

$$b = y_1 = 9102187917040423$$
$$c = -y_3 = 4183$$
$$a = \frac{c + (N + 1 - p - q)b}{e} = 9102187917040423$$

So that $ea - \phi(N)b = c$ with $a \approx N^{0.262}$. Also, we observe that $\frac{a}{b}$ is not a convergent of $\frac{e}{N}$. Moreover, all the convergents $\frac{a'}{b'}$ of $\frac{e}{N}$ with $a' < \frac{1}{3}N^{\frac{1}{4}}$ satisfy $|ea' - \phi(N)b'| > N^{-\frac{3}{4}}ea'$. This shows that the attack Blomer-May's work will not give the factorization of N.

5.5 Conclusion

In this study, the case that we have taken into consideration is when the RSA public parameter N with its corresponding exponent e which associated to the equation $ea - \phi(N)b = c$. Using Coppersmith's method, we have proved that RSA is unsecure if the parameters a, b, and c are suitably small. Moreover, we have shown that the famous bound $d < N^{0.292}$ of Blomer-May's work is a particular case of our attack. Thus, one needs to be cautious in choosing the public and private exponent in order to ensure that the cryptosystem is invunerable from attacks. Alternatively, Sun et al.[41] suggested that one could use an unbalanced primes as an attempt to avoid small decryption exponent attack.

[41] Sun, H. M., Yang, W. C., Laih, C. S. (1999). On the design of RSA with short secret exponent. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 150-164). Springer, Berlin, Heidelberg.

6 Chapter: Multi-criteria analysis as a new approach to decisions

6.1 From decision theory to decision aid theory; 6.2 Types of problems addressed by the MCDA; 6.3 Selection of the multicriteria method; 6.4 Detailed description of the multi-criteria analysis; 6.4.1 Phases of the formal structure of the multicriteria methodology; 6.5 Bibliometric analysis of multicriteria approaches.

6.1 From decision theory to decision aid theory

The structuring of complex decision-making problems has seen an evolution of the methodologies and mathematical modeling used in real contexts, evolving and defining new scenarios.

In the first section, the resolution of decision-making problems was mentioned by identifying the best practices of a better alternative that would be the optimal choice with respect to a set of different options. This theory, also called mainstream, is valid when we define a decision-making problem by assuming a rational agent as the decision-maker. However, from the analysis carried out, elements have emerged that lead the decision-maker to commit distortions in the decision-making process such as to

determine a new conception of a decision-maker that is no longer perfectly rational.

In the traditional formulation the decision-making problem is understood as a process within which one or more agents must support a choice between a set of alternatives respecting certain constraints and objectives. In this definition, the following characteristics can be identified which underlie the classical theory, ie a well-defined set of admissible alternatives; a single objective function that takes into account the preferences of the decision maker; a mathematical problem well formulated in terms of an objective function to be maximized or minimized respecting the constraints; the solution of the problem is configured in the alternative that maximizes or minimizes the objective function.

In this way the decision-making process is modeled by means of a single dimension, this determines an alteration of the complexity that occurs in real contexts, in this case we speak of a monocheterial approach which often reduces the analysis of a complex decision-making problem to simple calculations.

The decision taken following this methodology is identified by a single decision maker who expresses his preferences summarized by a single analysis criterion; in this way the evaluation of the different alternatives of the decision-making process takes place on the basis of the single criterion identified.

In formal terms, indicating with A the set of possible alternatives, with g a real-valued function defined in A that expresses the agent's preferences, the action a is preferred to the action b if $g(a) > g(b), \forall\, a, b \in A$; while the action b will be considered indifferent to the action a if $g(a) = g(b), \forall\, a, b \in A$.

This analysis can be effective in decision-making problems of a simple nature while it is not completely satisfactory in the formulation of real decision-making processes as there are various problems: the monocheterial approach describes all the quantities that come into play with the same unit of measurement and this in the reality is not always correct, furthermore carrying out an analysis totally based on a single criterion leads to the risk of excluding essential elements of the decision-making problem by inadequately formulating the model that leads to the definition of the solution.

The main method included in this methodology is the cost-benefit analysis which aims to calculate the economic convenience of a project and therefore does not consider elements that cannot be quantified and cannot be evaluated in monetary terms.

In this regard, it is essential to identify and define new models that make it possible to represent a "multi-dimensional" vision that is more suitable for solving real complex decision-making problems and supporting the decision-maker along the choice process.

In fact, there is an evolution of the classical models of decision theory which identifies a whole series of methods, methodologies, and tools suitable for the real context just highlighted.

In this way, the passage from a monochromatic approach is determined which uses linear optimization techniques with a single criterion, which does not lend itself to contexts where there are multiple objectives to be pursued at the same time, not perfectly quantifiable, imperfect elements and poor rationality; to a multicriteria approach, which envisages a plurality of objectives, several not perfectly rational decision makers can coexist with different points of view, allowing a breakdown of the object of

analysis into criteria for a more detailed analysis of the final objectives. Therefore from the classical theory of decisions we pass to a decision aid theory which, against the presumed perfect rationality of decision making, contrasts the greater flexibility and subjectivity of decision-making aid.

In this work the focus is placed on the methodology of multicriteria analysis, defined by the main author Roy as follows:

> "*When the heterogeneity of the consequences is such that the previous risks cannot be avoided, it is preferable to proceed with a multi-criteria analysis. The latter consists in making explicit a family of several criteria, each of which is suitable to represent a relatively homogeneous category of consequences*" (Roy 1993)[42].

Multicriteria analysis techniques fall within the context of decision making support methods.

More generally, Multi Criteria Decision Analysis can be defined as a discipline aimed at providing support to the decision maker in the analysis of a complex problem by comparing alternatives according to different criteria, in order to achieve a weighted choice in line with the set objectives.

In fact, in reality the decision-making problems are characterized by the presence of different points of view, by a plurality of objectives and by different evaluation criteria; from this point of view it is extremely difficult and sometimes impossible to find the optimal solution to the problem respecting all the relevant elements. In general, on the basis of this analysis, there is no one action that is better than all the others, in relation to all

---

[42]Roy, B., & Vanderpooten, D. (1996). The European school of MCDA: Emergence, basic features and current works. Journal of Multi - Criteria Decision Analysis, 5 (1), 22-38.

the criteria considered; therefore, the best result that can be obtained in this perspective is the search for a compromise solution (Roy, 1985.). For this reason, the concept of "optimal choice" is replaced by the concept of "compromise choice" based on the integrated analysis of several attributes.

It is important to underline the fundamental aspect of this tool: the analyst helps the decision maker through the multi-criteria methodology to structure an appropriate analysis for the decision problem, while maintaining complete control over the final decision.

This methodology is characterized by the definition of the decision-making process by structuring the objectives analyzed by separating them into criteria and alternatives. This translates into the preliminary activity of transforming the various objectives set in place by the decision maker into criteria, in order to subsequently be able to compare the various alternatives available.

In this context, the criteria are defined as the operational translation of the objectives: that is, they are quantitative or / and qualitative variables that measure the performance and impacts of the alternatives analyzed.

One of the significant elements of this method emerges from this definition: while in the theory of expected utility it is possible to consider only quantitative variables taking into account the probability of occurrence of the causal variable considered; and in general the standard theory takes into account only quantitative variables; the method introduced allows an evaluation analysis of the economic criteria that can be monetized and extra-economic criteria that can be measured in qualitative terms.

Mathematically, a criterion is a function defined on the set of alternatives that maps the comparison relationship between two alternatives with respect to a variable that describes the decision problem.

At the basis of this tool there is therefore a comparative evaluation of the various elements that allows to examine the decision-making problem at 360° since it takes into account the value assumed by the various alternatives as the decision criterion changes.

A choice evaluation technique is therefore implemented through the optimization of a vector of several criteria weighted by the preferences of the decision maker.

Let A be the set of possible alternatives $V = \{g_1(a), g_2(a), \dots, g_3(x)\}$ is a multicriteria choice vector, composed of the functions g_n that operate on the same choice set A.

Another main element of the multicriteria method is the alternatives, these represent the set of all the possible actions useful for solving a complex decision-making problem.

6.2 Types of problems addressed by the MCDA

The MCDA allows you to take on multiple decision objectives within a single decision process: the contextual and simultaneous analysis of multiple objectives allows you to analyze the problem as complex as possible in a faster way than the analysis of decision-making problems solved by classical approach.

In the literature, in relation to real problems that can be faced in decision-making contexts of any kind, multicriteria methods consider and solve problems taking into account four types of complex problems:

problem definition, ranking problems, sorting problem, and choice problems.

The definition of a decision-making problem consists in structuring and identifying acceptable and unacceptable alternatives valid for solving the problem based on the objectives that have been set up. This typology of decision-making problem can be considered as one of the phases of the decision-making process with respect to which the multicrterial analysis can represent a valid help. The ranking problems allow to define an ordering of the alternatives and thus to obtain a global priority of the same evaluated with respect to the criteria and the analysis objectives. Tackling a ranking problem also allows you to order a set of alternatives, among which the decision maker must proceed to make a choice; in this hypothesis the choice problems represent a category incorporated within the ranking problems. In general, the choice problems consist in the selection and identification of the best alternative or the subset of the best or satisfactory alternatives of the decision-making process. Another type of problem that can be solved through multi-criteria methodologies are the sorting problems, which consists in assigning each option to predefined categories; in fact, this decision support tool has the ability to classify alternatives into homogeneous and distinct classes. Two sub-categories are distinguished in relation to classification problems, taxonomy problem and ordinal classification: in the first, the values of the attributes and the predetermined classes in which to include the various options are not characterized by relations of preference; contrary to what happens in the problems of ordinal classification.

Furthermore, decision-making problems can be classified according to the different aspects as follows:

- in relation to alternatives in discrete or continuous problems (what is relevant is the finite or infinite number of options respectively);
- with respect to information in soft problems (if the information is qualitative), hard (quantitative information), mixed (qualitative and quantitative information);
- on the basis of the scenario, problems can be distinguished in conditions of certainty, risk, uncertainty or competitive uncertainty:
    - Faced with problems with deterministic and perfectly known a priori information we are in the context of problems in conditions of certainty.
    - The existence of probability distributions of known information are characteristic of problems under risk conditions.
    - In the absence of probability distributions, on the other hand, the category of problems occurs under conditions of uncertainty,
    - If we add to the previous one that the results are influenced by the decisions made by the "competitors" we speak of problems in conditions of competitive uncertainty (studied by game theory).

In the literature there are a plurality of multicriteria methodologies that can be classified within two macro-categories such as outclassing methods and hierarchical methods. the first class includes all those methods that adopt principles of dominance with respect to the evaluation of alternatives; while hierarchical methods are those that take into consideration the structuring and definition of a hierarchy for solving the problem.

Within the multiple criteria decision aid methodology there is a relationship of fundamental importance: the relationship of dominance.

In mathematical formulation the concept of dominance expresses the following relationship:

Give, $a, b \in A;\ aDb$ if and only if $g_j(a) \geq gj(b), \forall g_j \in G.$

Considering two options a and b belonging to the set of all possible alternatives A, we say that the action a dominates the action b if and only if the evaluation of a is greater than or equal to that b of on all the criteria with at least one of them strictly better. This is an objective relationship since it does not depend on a subjective evaluation that the agent attributes to the criteria.

A further characteristic of multi-criterion methods associated with the dominance relationship is the concept of efficient action: action $a \in A$ is considered efficient if and only if no other action of A dominates it. This highlights the hypothesis in which an alternative a is considered efficient if there is no other admissible option that is better at least in relation to one criterion without worsening the evaluation on at least one other criterion. The so-called Pareto optimal which represents the subset of A that groups all the efficient actions whose search is identified as a vector optimization problem falls within this perspective

These concepts are relevant in that they can simplify the analysis of a decision problem, for example, it is possible to exploit the concept of a set of efficient actions to select the best alternative within a choice problem; or to set up an ordering problem by means of a dominance relationship such that the action a will be identified at a higher level than the action $b\ if\ aDb$.

Tackling real decision-making problems through MCDA involves an aggregation procedure to exploit the dominance relationship and make all actions comparable with respect to the criteria considered.

there are different aggregation methodologies that can be used to solve a complex decision problem through multi-criteria analysis, among these we mention the main ones such as the weighted sum, the maximum, the minimum.

The method that is suitable for aggregating homogeneous variables that identify the same characteristic (example in contexts where the use of votes is required) is the weighted sum $W(x)$:

$$W(x) = \sum_{j=1}^{m} w_j g_j(x)$$

Where is it:

- $g_j(x)$ constitute the quantitative assessments on the criteria, with $g_j(x), j = 1 \ldots m$;
- w_j is the weight expressed in terms of importance associated with the criteria.

Using this method it is necessary that the evaluations are appropriately normalized in such a way as to obtain evaluations expressed in a single unit of measurement.

Therefore, it occurs:

$$\forall a, b \in A$$
$$aPb \Leftrightarrow W(a) > W(b)$$
$$aIb \Leftrightarrow W(a) = W(b)$$

Where a it is preferred to b if the value of the valuations with respect to the criteria of the share a is preferred to the value of the valuations of the share b, while in the case in which these valuations are equivalent then

the two shares are indifferent; these relationships identify a structure of preferences as a total pre-order.

In the event of a decision problem in which the shares are characterized by performance evaluations, the maximum or minimum value can be used. The aggregation procedure using the maximum value (example in terms of profits, profits) is obtained using the following formula:

$$M(x) = \underset{g_j \in G}{\text{Max}}\, g_j(x)$$

Where is it:

- by $x \in A$ means of any action belonging to the set of different alternatives;
- $M(x)$ represents the maximum rating associated with each action against the criteria g_j.

By obtaining the following preference structure:

$$\forall a, b \in A$$
$$aPb \Leftrightarrow M(a) > M(b)$$
$$aIb \Leftrightarrow M(a) = M(b)$$

As in the previous hypothesis, a complete pre-order is obtained and the evaluations are required to be expressed in the same unit of measurement.

Symmetrical aggregation method that identifies the shares based on the worst performance (example in terms of cost) is the determination of the minimum value:

$$m(x) = \min_{g_j \in G} g_j(x)$$

Where is it:

- by $x \in A$ means of any action belonging to the set of different alternatives;
- $m(x)$ represents the minimum rating associated with each action with respect to the criteria g_j.

As seen in the previous method, the preference structure of this approach also represents a complete pre-order and it is necessary to express the evaluations of the criteria using the same unit of measurement.

In the representation of the mathematical model useful for solving a complex problem, a measurement scale is often used within the multicriteria methodology. There are different types of measurement scales and the choice between these depends on the characteristics of the information to be extracted, therefore on the characteristics of the measured attribute.

The nominal scale is characterized by the property of uniqueness by which it is possible to identify a different label to the options observed with different intensity of the measured attributes. Using this type of scale, each survey element can be uniquely classified. The nominal scale has the following properties:

reflective: $A = A$

symmetrical: if $A = B \Rightarrow B = A$

transitive: if $A = B$ and $B = C \Rightarrow A = C$

The ordinal scale can be used when, in addition to the character of uniqueness, the property of ordering of numbers is manifested: this type of scale allows to identify ordinal relationships between the elements, thus constructing an ordering or ranking.

The interval scale allows you to operate with both continuous and discrete quantitative variables, you work with cardinal numbers, and in this case it is essential to set an arbitrary unit of measurement and an arbitrary zero. the temperature measured in degrees centigrade is an example of an interval scale.

Also the scale of the ratios allows to measure quantitative variables and foresees the use of cardinal numbers, in this case it is essential to identify an absolute 0 intended as a limit value with respect to which it is not possible to assume lower values. This type of scale is used to measure attributes through products or reports, for example to measure income[43].

6.3 Selection of the multicriteria method

In order to select the most suitable multi-criteria method for the decision-making problem, it is necessary to investigate the nature of the alternatives: in the case of alternatives of a continuous nature, the selection of a multi-criteria method will be oriented towards mathematical programming; in the case of alternatives of a discrete nature, it is necessary to carry out a further analysis with respect to the nature of the criteria, which can be qualitative or quantitative variables. In this regard, two types of methods are distinguished: multi-objective methods and multi-attribute methods. multi-objective methods seek the solution of an ideal compromise generally assuming that the problem to be solved can be schematized with a mathematical model and assume infinite solutions, therefore, this type of methods is used for the resolution of decision-making problems with the presence of continuous alternatives. In the case of discrete mathematics to a well-defined group of possible solutions, the multi-attribute methods constitute a valid support for the decision in many real cases in which the

[43] Stevens, S. S. (1946). On the theory of scales of measurement. *Science*, *103* (2684), 677-680.

number of alternatives is finite and the criteria are qualitative or quantitative.

In order to verify the correctness of the evaluation of the objectives of the problem, the multicriteria methods foresee the implementation of the sensitivity analysis. This verification can concern the method, the criteria, the weights. The sensitivity on the method makes it possible to verify the robustness of the method used: a different method is applied to the data and to the computation of the final scores to check the dependence of the results on the calculation method. the sensitivity on the criteria allows to study the behavior of the modeling with respect to the variation of the number of criteria within the method used. In particular, the analysis is carried out by adding or subtracting decisional criteria for the evaluation of the alternatives and verifying whether the behavior of the adopted scheme undergoes or not variations in the results. The sensitivity on the weights, the multi-criteria methods are constructed through interaction with the decision maker / expert in the sector, who expresses a preference order of the criteria in terms of judgments of merit; this verification allows to ascertain the degree of influence of each judgment on the final decision.

6.4 Detailed description of the multi-criteria analysis

The multicriteria analysis as highlighted by the examination of the previous paragraphs is the set of tools and methods that provide the mathematical methodology that incorporates the value of decision makers and stakeholders, as well as the technical information to select the best

solution for the problems and to take more logical and scientifically coherent decisions[44].

It is a technique of evaluation of the different objects of a whole (which constitute the alternatives) on the basis of a certain number of criteria with respect to which an agreement and a sharing has been established, between the actors involved (decision makers), within their nature and their relative importance (weights) are relevant. Each alternative is "measured" with reference to each criterion. Therefore, the clarification of all the components of the decision-making system (weights and objectives) occurs.

The use of MCDA concepts improves decision flexibility to meet the various requirements of different stakeholders or decision makers.

The Multiple-Criteria Decision Analysis (MCDA) is a research area within the field of Decision Analysis (DA), which aims to develop methods and tools to facilitate decision making, particularly in terms of choice, ranking or selection of options (i.e. alternatives, solutions, course of action, etc.), in the presence of several, and often conflicting, criteria[45]

In fact, this methodology also derives from the need to identify methods and tools capable of taking into account parameters that cannot be transferred in monetary terms.

Multi-criteria analysis establishes the preferences among the options in reference to an explicit set of objectives that the decision maker (which can be identified in an institution, an organization, a company and so on) has

---

[44]Linkov, I., & Moberg, E. (2011). Multi-criteria decision analysis: environmental applications and case studies. CRC Press.

[45] Zanakis et al. 1998; Figueira et al., 2005.

identified and for which he has established criteria (attributes) to evaluate the extent to which the objectives have been achieved.

The value that the MCDA provides us is therefore a function of the alternatives, of the criteria, we want to analyze in an integrated way several criteria that are also contrasting with each other (attributes-criteria relevant in the evaluation of alternatives) and of the objectives.

The main role of the techniques is to address the difficulties that decision makers have shown to have in managing large amounts of information, with multiple objectives, multiple evaluation variables to be taken into consideration, therefore faced with a complex decision-making problem and achieve a consistent solution.

A key feature of MCA is its emphasis on decision team judgment, setting goals and criteria, estimating weights of relative importance and, to some extent, judging the contribution of each option to each performance criterion.

It is a methodology where subjectivity is detected because in principle, the choices, criteria, weights and evaluations of the achievement of the objectives are made by the decision makers, although "objective" data can also be included.

From the literature it emerges that MCDA represents a decision support discipline that uses a series of methods and concepts that derive from different scientific theories and methodologies. It is therefore a set of methods that are also different from each other depending on the theoretical background to which they relate. In fact, the heterogeneity of the methods lends itself to the resolution of the most varied problems, and this heterogeneity is functional to the same heterogeneity of the problems encountered in reality.

It is necessary to consider how the methodology has certain characteristics that are common to the methods deriving from it, therefore many methods can be traced back to a single formal structure that can be described by means of a sequence of phases.

6.4.1 Phases of the formal structure of the multicriteria methodology.

In structuring a complex decision-making process, the first step to take is to understand whether or not to address the decision problem using a multi-criteria methodology. Choosing to perform the MCDA means that such analysis was deemed to provide relatively more value than using other methods.

The first real phase from the analysis with multiple criteria is the identification of the objective or more final objectives that determine the direction to follow. This phase is crucial for formulating the next phases, but this does not imply that these objectives remain fixed during the analysis, since as the process progresses, new issues and new elements emerge that can lead to a change or deviation from the objectives initially set.

The objective (s) must be established on the basis of the logic identified by the SMART acronym: Specific, Measurable, Achievable, Relevant, Defined over time.

In relation to the character of the specificities it is necessary to answer the following questions: What - What do I want to achieve? Why - Why is this goal important? Who - Who is involved? Where - Where is it? Which - What resources or limits are involved? The objective must be measurable, that is, it must be expressed or at least expressed in a certain unit of

measurement for evidence of the monitoring of progress and the actual achievement of the objective. Another characteristic is that it must be realistic and achievable, even if ambitious it must be commensurate with the available resources, skills and context. The character of relevance is useful to be in line with the mission of the "decision maker" (company, organization, company). Defined over time:

The first impact for the MCDA of these objectives is on the choice of key actors participating in the analysis: A key player is anyone who can make a useful and meaningful contribution to the MCDA. The key actors are chosen to represent all the important perspectives on the subject of the analysis. An important perspective is that of the final decision maker and the body to which that person is accountable. These people are often called, stakeholders, people, groups or organizations who have an interest, an investment, are influenced or can influence the consequences of any decisions made. No MCDA analysis is ever limited to just the perspective of the interested parties. Other key players participate because they possess knowledge and skills on the subject. This includes both subject to within the organization and often includes external experts who hold information that could aid the analysis. MCDA planners will need to consider all those who should be involved and the extent of their participation in the analysis.

We proceed with the design of the system and the multi-criteria model to be implemented in the decision-making process, this represents the most technical phase.

Describing the context in which you act also allows you to acquire further relevant information: with respect to the objectives to be achieved, the gap between the current condition and the vision for the future is identified.

Introduce relevant alternatives in the decision-making process into the analysis. The identification of the options considered significant, can be done through different tools, for example through the observation of the strengths, weaknesses, opportunities and threats of a SWOT analysis, considered particularly useful in the development of alternatives. As underlined for the determination of the objectives, also in this phase the progression of the process can highlight new information not previously evaluated such as to modify, subtract or add further potentially relevant alternatives.

We arrive at the introduction phase in the analysis of the criteria that express the different properties with which the alternatives create value.

As noted above, the methodology here may include:

- cardinal measures (e.g. measures of physical quantities)

-ordinals (rankings)

-nominal (direct expressions of preference judgments; example different degrees of judgments: sufficient-good-excellent).

The description of each alternative taking into account each evaluation criterion takes place through the performance matrix.

This represents the methodological tool that underlies the multi-criteria methods and is represented by a matrix also called decision-making matrix or evaluation matrix, which allows you to compare the alternatives with the criteria with respect to the main objective. The construction of this matrix takes place by inserting the alternatives along the rows, putting them in relation and evaluated with respect to the criteria to be inserted in the columns. The evaluation that emerges from the comparison represents the performance of the alternative with respect to the criterion considered with a view to achieving the main objective.

		Criteria			
		C_1	C_2	$C_{...}$	C_n
Alternatives	A_1	x_{11}	x_{12}	...	
	A_2	...	...		
	$A_{.}...$				
	A_m				x_{mn}

The key idea is to consider scales of measurement that represent the relative importance of the criteria with respect to the alternatives to be evaluated. Different types can be used, for example the numerical scale or the rating scale.

Then follows the attribution of the weights that represent the expression of the criteria / alternatives in terms of importance.

$$V = w_1 s_1 + w_2 s_2 + \cdots + w_n s_n = \sum_{i=1}^{n} w_i s_i \qquad i = \{1,2, \ldots n\}$$

The MCDA offers a number of ways to aggregate data on individual criteria to provide indicators of the overall performance of the options that allow to identify the alternative or set of "compromise" alternatives for the pursuit of the final goal (s).

Multiple criteria analysis has several advantages over informal judgment not supported by analysis:

- is open and explicit
- the choice of objectives and criteria that any decision-making group can take are open to analysis and change if deemed inappropriate
- Scores and weights, when used, are also explicit and are developed according to established techniques. They can also be referred to other sources of information on relative values and modified if necessary

- performance measurement can be subcontracted to experts, so it does not need to be left in the hands of the decision-making body itself
- can provide an important means of communication, within the decision-making body and, subsequently, between decision makers and the wider community, and
- scores and weights are used, provides an analysis audit trail.

6.5 Bibliometric analysis of multicriteria approaches

In various fields of study, scientific knowledge has grown considerably in recent years; to such an extent that the evaluation of literature represents an important research work in order to acquire and transmit this knowledge.

In this regard, an interesting systematic review of multi-criteria decisions can be examined through a bibliometric analysis in order to obtain a general picture of the global evolution of research on this methodology.

The analysis was carried out over the period from 1977 to 2022 on the bibliographic data reported by two main databases such as Scopus and Web of Science through a search on titles, abstracts, keywords and articles; this made it possible to acquire an overview of the research carried out on multi-criteria approaches.

What is the annual growth of scientific publications in multi-criteria decision-making methods? Which countries have the most significant production of articles on multi-criteria decision support methodology? What are the main research areas? Who are the most influential authors and researchers in the scientific research of multi-criteria decision-making methods? Which journals have the most publications? Which methods are most used? What are the conceptual structures of many criteria decision support methods?

In recent years, the volume of published articles has increased considerably also following the digitization of scientific journals, which is why a bibliometric analysis is more effective as it allows you to manage many documents more efficiently and to review related literature. In fact, when we talk about bibliometric analysis we refer to the quantitative study of bibliographic materials[46] that distinguish development in a research field.

Bibliometric literature review can be carried out through different techniques, the most used methodologies are social network analysis which is characterized by a network structure composed of nodes and existing relationships between them, represented by a graph; there are different types of biometric networks such as co-authorship networks[47],[48] bibliographic coupling networks[49] and co-citation networks[50]. Another relevant technique is co-word analysis, which allows to map the intensity of associations between the elements present in the text data through a co-occurrence analysis of the keywords, those that have a high relevance are

[46] Merigó, J.M.; Yang, J.-B. (2017). A bibliometric analysis of operations research and management science. *Omega*, *73*, 37–48.

[47] Barabási, A.L.; Jeong, H.; Néda, Z.; Ravasz, E.; Schubert, A.; Vicsek, T. (2002). Evolution of the social net-work of scientific collaborations. *Phys. A: Stat. Mech. Its Appl. 311*, 590–614.

[48] González-Alcaide, G.; Pinargote, H.; Ramos, J.M. (2020). From cut-points to key players in coauthorship networks: A case study in ventilator-associated pneumonia research. *Scientometrics*, *123*, 707–733.

[49] Yan, E.; Ding, Y. (2012). Scholarly network similarities: How bibliographic coupling networks, citation networks, co-citation networks, topical networks, coauthorship networks, and co-word networks relate to each other. *J. Am. Soc. Inf. Sci. Technol*, *63*, 1313–1326.

[50] Hernández, J.M.; Dorta-González, P. (2020). Interdisciplinarity Metric Based on the Co-Citation Network. *Mathematics*, *8*, 544.

grouped into specific clusters, each of which corresponds to a search theme[51],[52].

In the reference context, the latter method was used to conduct the bibliometric analysis inherent to the multi-criterial methods of decision support in the period from January 1977 to April-29-2022 by means of the co-occurrence analysis of specific research queries and limited to title, abstracts, keywords and articles. The search queries used were the following:

((“multi-attribute decision making” or “madm” or “mcda” or “modm” or “mcdm” or “multi-criteria” or “multi-criteria” or “multiplecriteria”) and (“ahp” or “todim” or “topsis” or “promethee” or “electre” or “vikor” or “maut” or “fitradeoff” or “dematel” or “copras” or “multimoora” or “swara” or “analytical network process” or “anp” or “simple multi-attribute rating technique” or “smart” or “goal programming” or “thor” or “cbr” or “saw” or “condorcet” or “drsa” or “macbeth” or “paprika” or “wpm” or “wsm” or “utadis” or “waspas”)).

The search and data extraction strategy was conducted using the R Bibliometrix tool, obtaining 23.494 bibliographic records as shown in the following figure:

[51] Cheng, B.; Wang, M.; Mørch, A.I.; Chen, N.S.; Spector, J.M. (2014). Research on e-learning in the workplace 2000–2012: A bibliometric analysis of the literature. *Educ. Res. Rev., 11*, 56–72.

[52] Leung, X.Y.; Sun, J.; Bai, B. (2017). Bibliometrics of social media research: A co-citation and co-word analysis. *Int. J. Hosp. Manag., 66*, 35–45.

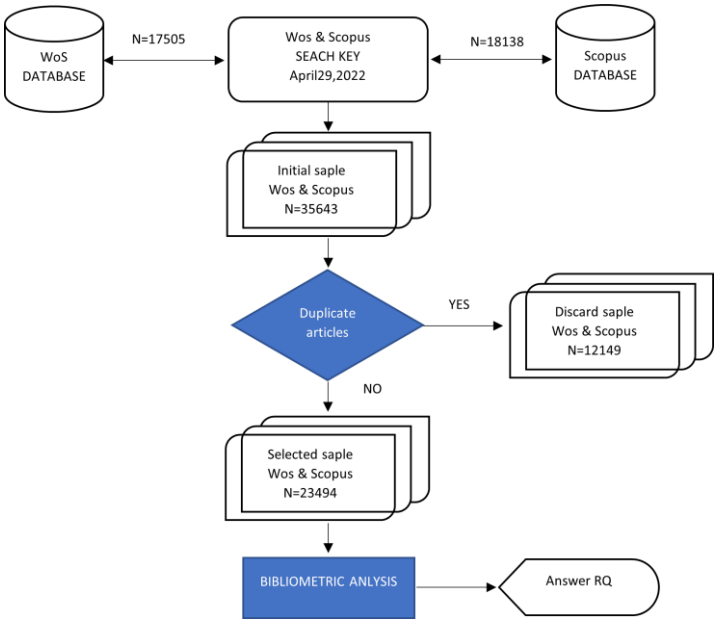


Figure 11:Search strategy and extraction of data. Source: Prepared by the authors based on Basilio et al.[53] *and Ghosh and Prasad*[54].

Relevant information emerged from the analysis carried out.

The temporal evolution of this study on the multi-criterion methodology recorded 1977 as the year of origin, the publishing process recorded the upward trend that began in 1986, in these first years there was an average number of annual publications of 7,3; value rose to 28,3 documents in the period from 1987 to 1996; subsequently the analysis identified a continuous growth of the average equal to 123,2 from 1997-2006, reaching a figure of 1.265,73 in the following years to date. In general, the annual percentage rate of increase in publications on the multi-criteria analysis was 14.18% for the entire analysis period.

This has led to a growing interest on the part of the scientific community for the multi-criteria approach in the topic of decision support.

---

[53] Basilio, M.P.; Pereira, V.; de Oliveira, M.W.C.M. (2021). Knowledge discovery in research on policing strategies: An overview of the past fifty years. *J. Model. Manag.*

[54] Ghosh, A.; Prasad, V.K.S. (2021). Off-grid Solar energy systems adoption or usage—A Bibliometric Study using the Bibliometrix R tool. *Libr. Philos. Pract.*, No Article 5673.

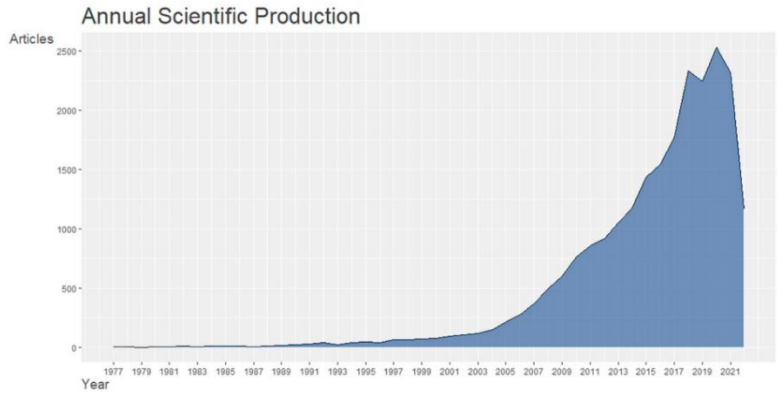


Figure 12: Graphical representation of the annual scientific production. Note: The data for 2022 corresponds to partial values quantified up to 29 April, 2022.

A further result that emerged from the analysis carried out concerns the monitoring of scientific production in the world. A contribution to research on multicriteria methods was recorded by 120 countries among which China represents the main country in terms of the number of equal to 18.50% of the entire scientific production, thus constituting a reference for the community.

The following are the top 10 countries that contribute most to scientific production in terms of methods with many criteria: China publications 4327, in second place we find India with 2485 publications followed by Turkey with 1788 publications; Taiwan 1192 United States 794 Brazil 752 Spain 608 Italy 555 and Malaysia 493.

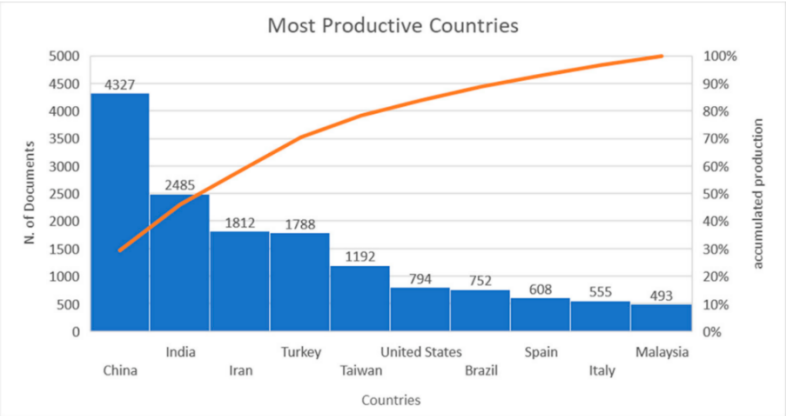


Figure 13: Graphical representation of the top 10 most productive countries.

Through the analysis of the co-authorship, the work made it possible to highlight the relationships between the main institutions involved in the research regarding the multi-criteria approach.

The research considered universities as a unit of analysis and whether it is based on specific criteria such as the minimum number of documents per organization≥50 and the minimum number of citations per organization≥50. The result of this analysis indicated that the main organizations involved are Islamic Azad University and Vilnius Gediminas Technical University.

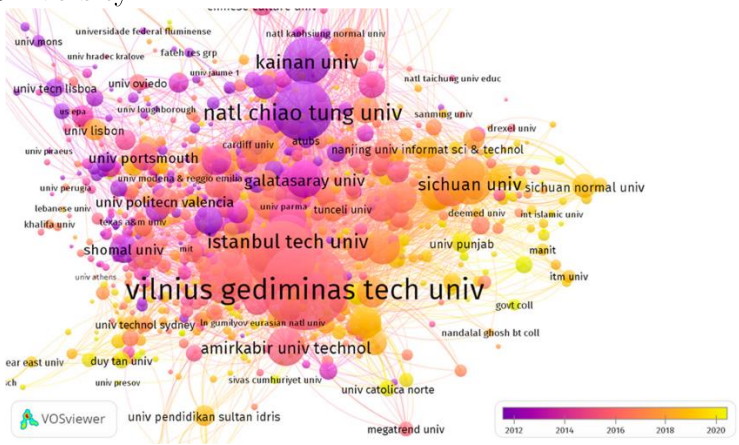


Figure 14: The network map of institutions involved in multi-criteria methods of decision-support research. Note: The colors of the circles are used to identify the clusters resulting from the analysis of the relations provided by the VOSviewer software.

The scope of application of the multi-criteria discipline may concern different thematic areas, which have undergone different attention over the years by the academic community. In particular, the first five research areas recorded in the examined time frame are highlighted. In the first period (1982-2002) the researchers focused scientific production in the field of operational research followed by business economics, information technology, engineering and mathematics. From 2003 to 2012 there was particular interest in the ecology of environmental sciences which with 288 articles takes the place of mathematics in the ranking, and for computer science which comes in second place, while scientific production in the field of operational research and business economics is reduced, falling to third and fourth place respectively. The last period records further changes, the

first five research areas are: engineering, computer science, ecology of environmental sciences, scientific technology and business economics.

Table 4: Evolution of scientific production according to research areas in the analyzed periods.

Research areas	Periods			
	1982 to 1992	1993 to 2002	2003 to 2012	2013 to 2022 (April 29)
	Ranking	Ranking	Ranking	Ranking
Engineering	4th	4th	1st	1st
Computer science	3rd	3rd	2nd	2nd
Environmental sciences ecology	-	-	5th	3rd
Science technology	-	-	-	4th
Business economics	2nd	2nd	4th	5th
Operations research	1st	1st	3rd	-
Mathematics	5th	5th	-	-

A further reference that emerges from the bibliometric analysis concerns the different multi-criteria techniques that have been introduced and which are in continuous evolution. The three methods most used in the application field and which have recorded the greatest scientific production are AHP, TOPSIS and VIKOR. The relationship between different techniques and different research areas was also observed and it emerged that 47% of multi-criteria methods support decision makers in the IT field (in particular the TOPSIS method), 35% are used in engineering (AHP prevails over other methods), 11% relate to business economics and 8% to operations research.

Table 5: Characteristics of the methods most used by researchers.

N	Method	Publication time	Recorded count	Research areas	Publication time (integrated/hybrid model)	Hybrid model	New technologies (machine learning)
1	AHP	1990–2021	6.835	Engineering (2.329)	1995–2021	1.388	38
2	TOPSIS	1991–2021	4.907	Computer science (1.797)	2003–2021	1.024	47
3	VIKOR	2002–2021	1.475	Computer science (519)	2009–2021	416	5
4	PROMETHEE	1989–2021	1.382	Engineering (445)	2001–2021	202	16
5	ANP	2000–2021	1.262	Engineering (428)	2006–2021	488	10
6	ELECTRE	1991–2021	1.005	Computer science (331)	2003–2021	120	6
7	DEMATEL	2007–2021	888	Computer science (289)	2007–2021	476	5
8	GOAL PROGRAMMING	1983–2021	553	Operations research (202)	1993–2021	147	3
9	SAW	1997–2021	403	Engineering (137)	2007–2021	67	5
10	TODIM	1999–2021	306	Computer science (171)	2013–2021	56	2
11	COPRAS	2006–2021	294	Business economics (83)	2011–2021	100	2
12	WASPAS	2012–2021	214	Engineering (68)	2013–2020	67	0
13	MULTIMOORA	2011–2021	198	Computer science (75)	2011–2021	43	0
14	SWARA	2011–2021	181	Business economics (46)	2011–2021	90	1
15	MAUT	1984–2021	164	Engineering (56)	2007–2021	19	0
16	MACBETH	1999–2021	162	Computer science (47)	1999–2021	27	0
17	WSM	1994–2021	87	Engineering (29)	2014–2021	17	2
18	DRSA	2002–2021	85	Computer science (51)	2012–2021	20	4
19	WPM	1997–2021	57	Computer science (23)	2014–2021	7	0
20	CBR	1996–2021	40	Computer science (25)	2006–2020	10	1
21	CONDORCET	1999–2021	35	Business economics (9)	-	0	1
22	FITRADEOFF	2016–2021	29	Computer science (14)	-	0	0
23	UTADIS	1998–2020	27	Operations research (14)	2005–2016	2	0
24	SMART	1996–2021	22	Engineering (9)	2021	2	0
25	PAPRIKA	2014–2021	12	Computer science (4)	2020	1	0
26	THOR	2008–2021	5	Engineering (2)	-	0	0

In recent years, attention has been paid to the possibility of developing methodologies that use hybrid models; by integrating multi-criteria methods with other methodologies such as, for example, machine learning techniques, it will be possible to increase the potential of these tools to support the decision-making process.

7 Chapter: Variation of the AHPSort model through the analysis of predictive models of Machine Learning

7.1 Introduction; 7.2 Review of the literature; 7.2.1 Analytic Hierarchical Process (AHP); 6.3 Methods; 7.4 Conclusion.

7.1 Introduction

Decision analysis at any level can be implemented by building new models. In particular the forecast of useful observations can prove to be an extremely analysis in decision making at the level.

For this purpose, this article proposes a new methodological approach to the AHPSort method, namely AHPSort-ML based on the implementation of Machine Learning that uses predictive analysis models.

Specifically, as described in chapter 2, Machine Learning explores the study and analysis of data based on the assumption that systems learn from data, propose predictions and based on these I can make decisions 'autonomously'.

For this reason it is believed that it may be useful to introduce a hybrid model to support the decision-making process in the formulation of complex problems characterized by multiple attributes, alternatives and different

points of view with the aim of obtaining a specific output with subsequent forecast analysis in the context of the classification.

The work proposed below is a "theoretical consideration" of an ongoing research with possible future developments and possible food for thought for further scientific research in the field of decision theory with a hybrid approach to modern "intelligent theories".

7.2 Review of the literature

The decision-making process can be characterized by multiple elements, in the situation in which a decision-making problem is characterized by multiple and contrasting criteria, one of the most suitable tools for decision-making analysis and the multi-criteria method.

The MCDA, as described in the previous chapter, is considered a multidisciplinary science that includes various decision-making tools related to this methodology but suitably characterized by distinctive elements useful in relation to the different decision-making scenarios but with common characteristics.

Among the most widespread methods is the Analytic Hierarchical Process (AHP) as an analytical method of decision support based on a multi-criteria approach.

7.2.1 Analytic Hierarchical Process (AHP)

The Theory of Analytical Hierarchy Decision Making (AHP) was developed by mathematician Thomas L. Saaty[55]: this method is characterized in the modeling of the complex problem by means of a hierarchical structure that allows to break down a problem characterized by elements of complexity and to obtain the final result through the detailed analysis of the various hierarchical levels.

The analytical approach to the decision through the method just introduced follows a series of good phases that start from the structuring of a hierarchical or a network structure, proceed in the comparison in pairs in terms of measure of relative importance between the actions and/or alternatives in relation to the higher level criterion in order to establish the relationships that articulate the structure of the decision problem.

The hierarchy branches from the final objective of the decision to the last level which is occupied by the different alternatives: each object of a higher level is related to two or more objects of a lower level.

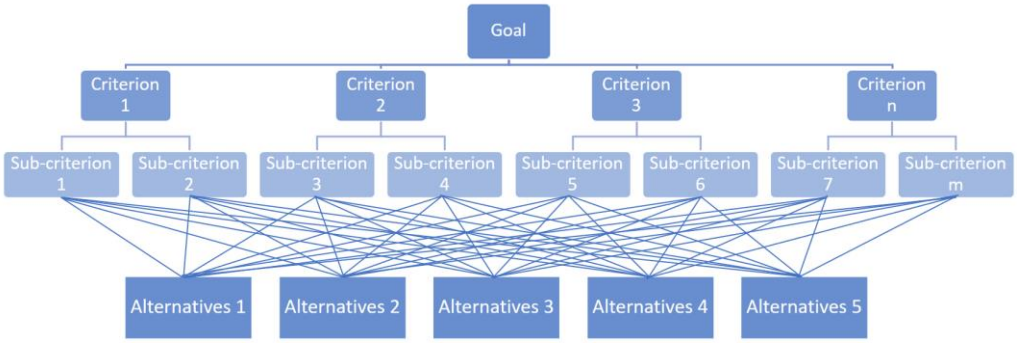


Figure 15: Hierarchical structure of the decision-making process with the AHP method.

[55] Thomas L. Saaty is considered one of the most relevant pioneers in the search for tools to support decision making.

The objects of a level can be grouped into "clusters" (eg groups of criteria) and from figure 6 it is evident that this approach therefore allows to bring each object, element, attribute back to the main objective.

At the basis of the modeling of a decision-making problem in the AHP methodology there are three characterizing principles: the principle of decomposition, identified in the "subdivision" of a complex process in all its constituent elements by means of a hierarchical structure; the principle of comparison, implemented through pairwise comparisons of the different elements; and the principle of the synthesis of priorities, understood in terms of defining a ranking through the clarification of global and relative priorities.

This specific multi-criteria approach is structured through a specific process that the decision maker has to design.

- First, the objectives of the project must be identified and analyzed.
- Establish pairwise comparisons of criteria.
- Define the matrix of the comparison judgment.
- Calculate relative priorities.
- Calculate the average value of priorities.
- Define the Random Index values that is the random index, the consistency index is the consistency ratio. If the consistency ratio is greater than 10%, yes redefines the comparison in pairs, otherwise one proceeds by establishing the complete table of comparison criteria.
- The analysis is carried out in the same way, first of sub-criteria and then of alternatives (therefore the comparison in pairs of the

complete matrix with the global aggregation) until the expression of the best decision is reached.

In determining the pairwise comparison, this procedure takes place through the use of a numerical scale that allows to quantify the dominance of one alternative over another in relation to each criterion or attribute screened. In the theoretical treatment of the AHP method, the author has introduced a special evaluation scale consisting of 9 grades of judgment called the Saaty Comparison Scale.

Table 6: Saaty scale of comparison.

Intensity	Judgement	Interpretation
1	Equal importance	The two elements contribute equally to the achievement of the objective
2	Weak importance	Intermediate judgment between 1 and 3
3	Moderate importance	The first element slightly dominates the second
4	More than moderate importance	Intermediate judgment between 3 and 5
5	Strong importance	The first element dominates the second
6	More than strong importance	Intermediate judgment between 5 and 7
7	Very strong importance	High dominance of the first element over the second
8	Remarkably strong significance	Intermediate judgment between 7 and 9
9	Extreme importance	Maximum degree of dominance of the first element over the second

A fundamental element of this hierarchical model consists in the introduction of the verification of the consistency of the judgments expressed by the decision maker. This verification takes place using specific indices:

Consistency Index. It allows to measure the possible inconsistencies in the evaluations and its value is obtained from the following formula:

$$CI = \frac{\lambda_{max} - n}{n - 1}$$

Where is it:

- λ_{max} is the maximum eigenvalue
- n is the number of elements to be analyzed (eg the number of criteria or sub-criteria or alternatives).

Radom Index. It is the value of inconsistency[56]of judgments attributed to a causal decision maker.

Order of the matrix	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RE	**0.00**	**0.00**	**0.58**	**0.90**	**1.12**	**1.24**	**1.32**	**1.41**	**1.45**	**1.49**	**1.51**	**1.49**	**1.56**	**1.57**	**1.59**

[56]Author Saaty created such a scale of predetermined values by conducting random judgments for a large number of replicates. Saaty, TL (1990). The Analytic Hierarchy Process-planning, priority setting, resourse allocation. RWS Publications, Pittsburgh.

The values entered in each cell of the table above are obtained from the average of the indices calculated at each replication for a large number of matrices having a square dimension[57].

Consistency Ratio: The consistency index must be compared with the random inconsistency to identify an acceptable or unacceptable evaluation.

$$CR = \frac{CI}{RI}$$

This value must not exceed 10% for the decision maker in question to be considered consistent. In the event that the CR exceeds the limit[58]imposed, a comparison between the analyst and the decision maker is considered useful for a review of the judgments assigned in order to obtain an acceptable level of inconsistency.

7.3 Methods

The method proposed in this work consists in the implementation of the AHPSort multicriteria method and the analysis of predictive models of Machine Learning to give life to a new approach.

---

[57]The table shown was generated by expert research from Oak Ridge National Laboratory and the Wharton School. The values were obtained by estimating 500 positive, square, reciprocal and random matrices from an order of 1 to an order of 15.

[58]In the recent analysis, the limits of the value assumed by the CR index so that the judgments expressed by the comparisons can be considered sufficiently consistent are:

- CR <5% for n = 3;
- CR <9% for n = 4;
- CR <10% for n> 4.

The AHPSort model aims to sort the alternatives into classes from least to most preferred, following a particular procedure. The first step consists in defining the decision problem by identifying the objectives, criteria and alternatives of the established problem. This is followed by the determination of the classes, where the profile of each class is delimited by the local profiles or is defined by the local central profiles. We proceed with the evaluation using the eigenvalue method, after having prioritized the importance of each criterion by means of the attribution of the weights by the experts, we first calculate the local priority for each alternative and by aggregating these weighted values we obtain the priority global for each alternative.

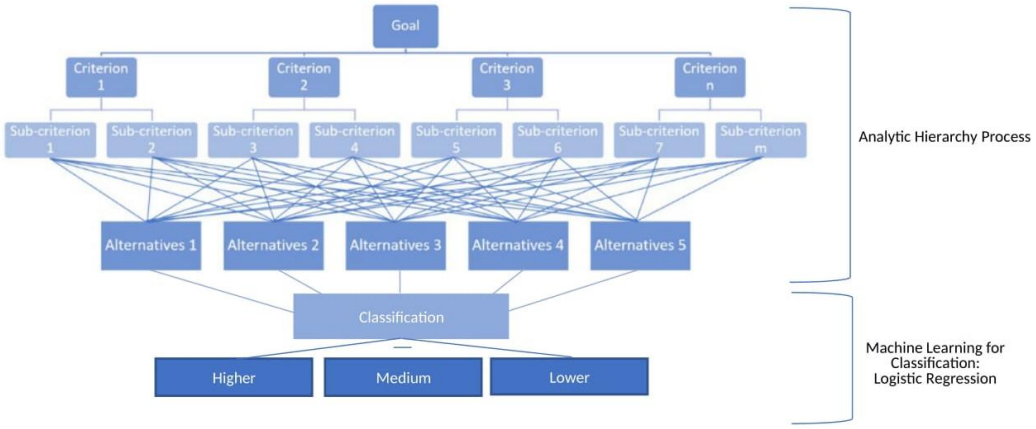
This article modifies the previous algorithm, in particular in the definition of the membership classes of each alternative.

In this work we introduce the determination of the classes through the analysis of predictive models of Machine Learning. The use of the supervised learning category is suitable for the purpose of the analysis, based on the type of output to be obtained, the attention is focused on the classification models since it is based on qualitative variables (categories).

In fact, in our study we are dealing with qualitative values since the distinction of classes occurs through a linguistic descriptor (high, medium, low or optimal, good, sufficient) not through numbers.

The goal is to create a model that can predict the target of a new observation based on the predictors.

The following graph illustrates how the hierarchical structuring of the decision problem takes on a new design:



Graphic 16: AHP-Sort -Machine Learning

With the new approach proposed, the classification can be done through logistic regression.

Logistic regression does not directly identify the class to which an observation belongs but predicts its probability. From a formal mathematical point of view, this algorithm uses the so-called logistic function to describe the probability of having a certain class 'y', given certain values for the inputs 'x':

$$py\,(x\,) \;=\; logistic\;function(x\,)$$

The logistic function has the property of always being included in the interval 0 and 1, whatever the value of x is. It is constructed using the exponential function and, in the case of a single predictor, it is written:

$$p(x) \;=\; \frac{e^{\beta_0+\beta_1 x_1}}{1 \;+\; e^{\beta_0+\beta_1 x_1}}$$

By manipulating the previous formula through logarithmic transformation in order to make the relationship linear, the following formula is obtained:

$$\log\left(\frac{p(x_1)}{1-p(x_1)}\right) = \beta_0 + \beta_1 x_1$$

Since the exponential function leads to excessively large results that even the system would have difficulty processing, this is why data analysts apply this logarithmic function. In particular, this formula actually represents a linear regression, for the function reported on the left hand side, which is called log-odds or logit. By means of this calculation we want to obtain the best straight line that approximates the observations, in order to attribute the various alternatives to their respective classes.

The method of Maximum likelihood is used to calculate the coefficients of the model, it is the method of maximum likelihood. This method is used as a criterion for choosing the parameters of the model β_0 and β_1 and such that the estimated probability that an observation is of a certain class is as close as possible to the category actually observed.

This statistical method is rigorously based on the maximization of the likelihood function:

$$l(\beta_0\, e\, \beta_1) = \prod_{i:y_i=1} p(x) \prod_{j:y_j=1} [1-p(x)]$$

Where is it:

- $\prod_{i=y_i=1} p(x)$ - productive of all values $p(x)$ calculated on all observations of such that $y_i = 1$; represents the probability calculated on all observations belonging to the category labeled with 1;
- $\prod_{j:y_j=1}(1-p(x))$- productivity of all values $(1-p(x))$ calculated on all observations of j such that $y_j = 0$, represents the probability calculated on all observations belonging to the category labeled with 0. rational

An important aspect in this context is the predictive capacity of the model. To evaluate this ability, the index is calculated based on the evaluation of the percentage error reduction.

$$Predictive\ efficiency = \frac{(errors\ without\ the\ model) - (errors\ with\ the\ model)}{(errors\ without\ the\ model)}$$

It is possible to notice that a machine learning model for solving a classification problem with logistic regression allows to structure predictions in the presence of a single predictor and a single variable.

In the case of complex models in which there are several variables, it is possible to extend the analysis by means of multiple logistic regression, whose function is the following:

$$p(x) = \frac{e^{\beta_0+\beta_1 x_1+\cdots+\beta_p x_p}}{1 + e^{\beta_0+\beta_1 x_1+\cdots+\beta_p x_p}}$$

Where is it:

- p indicates the index of the p different predictors,
- x represents the vector of all predictors.

This function continues to enjoy the properties of the regression function, this allows us to calculate the logarithm:

$$\log\left(\frac{p(x_1)}{1-p(x_1)}\right) = \beta_0 + \beta_1 x_1 + \cdots + \beta_p x_p$$

In the case of a situation of a multiple logistic regression situation the logit allows to obtain a multiple linear regression.

7.4 Conclusion

The work presented aims to be a theoretical treatment of the issue of complex decision problems using valid decision support tools such as multi-criteria analysis and machine learning.

In particular, a hybrid solution is proposed for the problem of classification of alternatives through a combined approach with the AHP method and Machine learning with the logistic regression algorithm.

The analytical hierarchical analysis method is used in the early stages of the decision-making process for determining the ranking of alternatives based on the main analysis objective. The Machine Learning algorithm is introduced for the classification in specific categorical groups in such a way as to identify, each time a new variable is introduced, the prediction about the belonging of the alternatives to the different classes.

The proposed methodological analysis can be a valid basis for future insights into decision support systems.

Final remarks

The careful analysis of the decision-making process has highlighted the fundamental role of information as an essential resource to better support decision making.

The literature excursus has created a gap for the decision maker to acquire a perfect knowledge of the observed phenomena, determined by the presence of a large amount of data, and incomplete and nuanced information.

From this research arises the need to deepen the knowledge of tools useful to the decision maker to overcome these limits, in particular the attention was placed for the first part of the research on fuzzy analysis and on a Machine Learning architecture: with hybrid fuzzy differential equation tools implemented with Artificial Neural Networks (ANNs) it was possible to manage the uncertainty due to incomplete information, which appears in many decision analysis models, allowing a better description of real world phenomena.

Further attention was paid to information security, to ensure the protection of the element that underlies the decision making process. In this scenario, cryptanalysis plays an important role, and in particular a comparison of the results of cryptography with the public parameter RSA was proposed in the report.

During the research activity, the importance of considering multiple evaluation elements in order to make decisions emerged, which led to a careful study of Multicriteria Decision Analysis. It has been demonstrated how the MCDA discipline represents a valid decision support and its

implementation with Machine Learning elements can be a valuable tool of advantage.

Bibliography

Agnoli, P., & Piccolo, F. (2008). *Probabilità e scelte razionali: una introduzione alla scienza delle decisioni*. Armando editore.

Barabási, A.L.; Jeong, H.; Néda, Z.; Ravasz, E.; Schubert, A.; Vicsek, T. (2002). Evolution of the social net-work of scientific collaborations. *Phys. A: Stat. Mech. Its Appl. 311*, 590–614.

Basilio, M. P., Pereira, V., Costa, H. G., Santos, M., & Ghosh, A. (2022). A Systematic Review of the Applications of Multi-Criteria Decision Aid Methods (1977–2022). Electronics, 11(11), 1720.

Basilio, M.P.; Pereira, V.; de Oliveira, M.W.C.M. (2021). Knowledge discovery in research on policing strategies: An overview of the past fifty years. *J. Model. Manag.*

Bede, B. (2008). Note on numerical solutions of fuzzy differential equations by predictor corrector method. Inform. Sci. **178**, 1917–1922

Blömer, J., & May, A. (2004, March). A generalized Wiener attack on RSA. In *International Workshop on Public Key Cryptography* (pp. 1-13). Springer, Berlin, Heidelberg.

Boneh, D., & Durfee, G. (2000). Cryptanalysis of RSA with private key d less than N/sup 0.292. *IEEE transactions on Information Theory*, *46*(4), 1339-1349.

Buckley, J. J., & Feuring, T. (2000). Fuzzy differential equations. *Fuzzy sets and Systems*, *110* (1), 43-54.

Caporarello, L., & Pennarola, F. (2006). Decision Support System e comportamento decisionale dell'attore organizzativo: alternanza tra

modello razionale ed euristico. ("Decision Support System e comportamento decisionale dell'attore ...") In Organizzazione, regolazione e competitività. Università degli Studi di Salerno.

Casasnovas, J., Rossello, F.: Averaging fuzzy biopolymers. Fuzzy Set Syst. **152**, 139–158 (2005).

Cheng, B.; Wang, M.; Mørch, A.I.; Chen, N.S.; Spector, J.M. (2014). Research on e-learning in the workplace 2000–2012: A bibliometric analysis of the literature. *Educ. Res. Rev.*, *11*, 56–72.

Coppersmith, D. (1997). Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of cryptology*, *10*(4), 233-260.

Coron, J. S. (2004, May). Finding small roots of bivariate integer polynomial equations revisited. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 492-505). Springer, Berlin, Heidelberg.

Cravera, A. (2020). Allenarsi alla complessità: schemi cognitivi per decidere e agire in un mondo non ordinato. ("Allenarsi alla complessità. Schemi cognitivi per decidere e agire in un ...") EGEA spa.

Damasio, A. R. (1995). L'errore di Cartesio, Adelphi edizioni, Milano.

De Finetti Bruno. (1970). Teoria della probabilità. Sintesi introduttiva con appendice critica. Volume primo.

de FSM Russo, R., & Camanho, R. (2015). Criteria in AHP: a systematic review of literature. *Procedia Computer Science*, *55*, 1123-1132.

De Gandt, F. (2006, June). Geometry and experience: Einstein's 1921 work and Hilbert's axiomatic system.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644-654.

Druckman, J. N. (2001). Evaluating framing effects. *Journal of economic psychology*, *22*(1), 91-101.

Ehrgott, M., & Figueira, J. (2010). *Trends in multiple criteria decision analysis* (Vol. 6, pp. 10-34). S. Greco (Ed.). New York: Springer.

Erodoto. «Storie, libro VII,10.».

Feng, G., & Chen, G. (2005). Adaptive control of discrete-time chaotic systems: a fuzzy control approach. *Chaos, Solitons & Fractals*, *23*(2), 459-467.

Finlay, P. N. (1994) Introducing decision support systems, Oxford, UK Cambridge, Mass., NCC Blackwell, Blackwell Publishers ("(PDF) Microstatistics and the Decision Support System in the Local ...").

Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge University Press.

Ghosh, A.; Prasad, V.K.S. (2021). Off-grid Solar energy systems adoption or usage - A Bibliometric Study using the Bibliometrix R tool. *Libr. Philos. Pract.*, No Article 5673.

González-Alcaide, G.; Pinargote, H.; Ramos, J.M. (2020). From cut-points to key players in coauthorship networks: A case study in ventilator-associated pneumonia research. *Scientometrics*, *123*, 707–733.

Gordon, Buchanan & Tullock. (1962). The Calculus of Consent: Logical Foundations of Constitutional Democracy.

Greco, Matarazzo, Slowinski. (2001). «Rough Sets Theory for Multicriteria Decision Analysis.» Article in European Journal of Operational Research,

Hernández, J.M.; Dorta-González, P. (2020). Interdisciplinarity Metric Based on the Co-Citation Network. *Mathematics*, *8*, 544.

Herrmann, M., & May, A. (2010, May). Maximizing small root bounds by linearization and applications to small secret exponent RSA. In *International Workshop on Public Key Cryptography* (pp. 53-69). Springer, Berlin, Heidelberg.

Hinek, M. J. (2009). *Cryptanalysis of RSA and its variants*. Chapman and Hall/CRC.

Hoffstein, J., Pipher, J., Silverman, J. H., & Silverman, J. H. (2008). *An introduction to mathematical cryptography* (Vol. 1). New York: springer.

Howgrave-Graham, N. (1997, December). Finding small roots of univariate modular equations revisited. In *IMA International Conference on Cryptography and Coding* (pp. 131-142). Springer, Berlin, Heidelberg.

Huz, S., Andersen, D. F., Richardson, G. P., & Boothroyd, R. (1997). A framework for evaluating systems thinking interventions: an experimental approach to mental health system change. *System Dynamics Review: The Journal of the System Dynamics Society*, *13*(2), 149-169.

IBM Global AI Adoption Index (2022). New research commissioned by IBM in partnership with Morning Consult.

IBM Institute for Business Value (2009), Capitalizing on Complexity Insights from the Global Chief Executive Officer Study.

Jerković, V. M., Mihailović, B., & Malešević, B. (2017). A new method for solving square fuzzy linear systems. In *Advances in Fuzzy Logic and Technology 2017* (pp. 278-289). Springer, Cham.

Jochemsz, E., & May, A. (2006, December). A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 267-282). Springer, Berlin, Heidelberg.

Kaleva, O.: Fuzzy differential equations. Fuzzy Sets Syst. **24**, 301–317 (1987).

Kamel Ariffin, M. R., Abubakar, S. I., Yunos, F., & Asbullah, M. A. (2018). New cryptanalytic attack on RSA modulus N= pq using small prime difference method. *Cryptography*, *3*(1), 2.

Keen, P. & M. S., Morton (1978) Decision support system: An organizational perspective. Reading, MA, Addison-Wesley Publishing Co

Kumar, R. S., Narasimham, C., & Setty, S. P. (2012). Generalization of Boneh and Durfee's Attack for Arbitrary Public Exponent RSA. *International Journal of Computer Applications*, *49* (19).

Lakshmikantham, V., Liu, X.Z. (1998). Impulsive hybrid systems and stability theory. Dyn. Syst. Appl. **7**, 1–10.

Lakshmikantham,V., Mohapatra, R.N. (2003). Theory of fuzzy differential equations and inclusions.Taylor and Francis, London.

Lanzi, D. (2007). Introduzione alla Teoria della Scelta Razionale. *Dip. di Scienze Economiche, Facoltà di Economia, Università degli Studi di Bologna.*

Lenstra, A. K., Lenstra, H. W., & Lovász, L. (1982). Factoring polynomials with rational coefficients. *Mathematische annalen*, *261*(ARTICLE), 515-534.

Leung, X.Y.; Sun, J.; Bai, B. (2017). Bibliometrics of social media research: A co-citation and co-word analysis. *Int. J. Hosp. Manag., 66*, 35–45.

Linkov, I., & Moberg, E. (2011). Multi-criteria decision analysis: environmental applications and case studies. CRC Press.

Liu, Y., Eckert, C. M., & Earl, C. (2020). A review of fuzzy AHP methods for decision-making with subjective judgements. *Expert Systems with Applications*, *161*, 113738.

May, A. (2003). *New RSA vulnerabilities using lattice reduction methods* (Doctoral dissertation, University of Paderborn).

Merigó, J.M.; Yang, J.-B. (2017). A bibliometric analysis of operations research and management science. *Omega*, *73*, 37–48.

MIMEO 2020: Greco Salvatore. «Webinar: La complessità del decidere ai tempi del COVID 19.» Università degli Studi Mediterranea di Reggio Calabria.

Mondin, B. (1968). La logica di S. Tommaso d'Aquino. *Rivista di Filosofia Neo-Scolastica*, *60*(2/3), 261-271.

Morin, E. (1993). La sfida della complessità. La sfida della complessità, 17-19.

Otadi, et al. (2017). Advances in Fuzzy Logic and Technology.

Pederson, S., Sambandham, M. (2009). Numerical solution of hybrid fuzzy differential equation IVPs by a characterization theorem. Inform. Sci. **179**, 319–328.

Roy B. (1981). The Optimisation Problem Formulation: Criticism and Overstepping. Journal of the Operational Research Society, 32, 427-436.

Seikkala, S.: On the fuzzy initial value problem. Fuzzy Sets Syst. **159**, 319–330 (1987).

Simon, H. A. (1950). Administrative behavior (p. 125). New York: Macmillan.

Simon, H. A. (1955) A Behavioral Model of Rational Choice, Quarterly Journal of Economics (69); trad it. 1985, Un modello comportamentale di scelta razionale, in Causalità, razionalità, organizzazione, Bologna, Il Mulino.

Simon, H. A. (1991). The architecture of complexity. In Facets of systems science (pp. 457-476). Springer, Boston, MA.

Stevens, S. S. (1946). On the Theory of Scales of Measurement. Science, New Series, Vol. 103, No. 2684 (Jun. 7, 1946), pp. 677-680.

Turban, E. (1995) Decision support and expert systems: management support systems, Englewood Cliffs, N. J., Prentice Hall.

Vaidya, O. S., & Kumar, S. (2006). Analytic hierarchy process: An overview of applications. *European Journal of operational research*, *169*(1), 1-29.

Weinberg, G.M. (1975) An Introduction to General Systems Thinking, New York, John Wiley ("references on systems theory | Biomatrix Systems Theory").

World Economic Forum. (2020). The future of jobs report 2020. Retrieved from Geneva.

World Economic Forum. (2022). The Global Risks Report 2022, 17th Edition.

Yan, E.; Ding, Y. (2012). Scholarly network similarities: How bibliographic coupling networks, citation networks, co-citation networks, topical networks, coauthorship networks, and co-word networks relate to each other. *J. Am. Soc. Inf. Sci. Technol*, *63*, 1313–1326.

Zanakis, S. H., Solomon, A., Wishart, N., & Dublish, S. (1998). Multi-attribute decision making: A simulation comparison of select methods. European journal of operational research, 107(3), 507-529.

Zhang, H., Liao, X., Yu, J. (2005). Fuzzy modeling and synchronization of hyperchaotic systems. Chaos Soliton Fract. **26**, 835–843.

TABLE INDEX

INDEX CHARTS

INDEX FIGURE