Journal of Artificial General Intelligence 6(1) 130-149, 2015
DOI: 10.1515/jagi-2015-0007
Submitted 2015-05-18
Accepted 2015-11-19

# On Mathematical Proving[1]

**Petros Stefaneas** petros@math.ntua.gr
*National Technical University of Athens*
*School of Applied Mathematical and Physical Sciences*

**Ioannis M. Vandoulakis** i.vandoulakis@gmail.com
*The Hellenic Open University*
*School of Humanities*

**Editor:** Tarek R. Besold, Kai-Uwe Kühnberger, Tony Veale

## Abstract

This paper outlines a logical representation of certain aspects of the process of mathematical proving that are important from the point of view of Artificial Intelligence. Our starting-point is the concept of *proof-event* or *proving*, introduced by Goguen, instead of the traditional concept of mathematical proof. The reason behind this choice is that in contrast to the traditional static concept of mathematical proof, proof-events are understood as processes, which enables their use in Artificial Intelligence in such contexts, in which problem-solving procedures and strategies are studied.
We represent proof-events as problem-centered spatio-temporal processes by means of the language of the calculus of events, which captures adequately certain temporal aspects of proof-events (i.e. that they have *history* and form *sequences of proof-events* evolving in time). Further, we suggest a "loose" semantics for the proof-events, by means of Kolmogorov's calculus of problems. Finally, we expose the intented interpretations for our logical model from the fields of automated theorem-proving and Web-based collective proving.

**Keywords:** mathematical proof, proof-event, problem solving, agents, calculus of events, Kolmogorov's calculus of problems, Polymath project, T. Gowers, J. Goguen, R. Kowalski, A.N. Kolmogorov.

## 1. Proofs as Facts vs. Proofs as Processes

Philosophy of mathematics during the first half of the twentieth century was largely centred on the concepts of mathematical *proof* and mathematical *fact* (corresponding to *truth*) as they were explicated within the major foundational programs and their associated logical semantics. From this standpoint, mathematical knowledge is viewed as a collection of logical systems that could capture in different ways certain aspects of the fundamental mathematical concepts (such as natural number) and the identification of the necessary mathematical principles (axioms). This tendency has achieved significant contributions to mathematical logic and foundational studies.

On the other hand, studies in history of mathematics have shown that the concept of mathematical proof has undergone significant changes. The Greek concept of *apodictic proof*, as exemplified by *geometrical demonstration* in Euclid's *Elements*, was replaced during the $17^{th}$-$18^{th}$

1 Both authors contributed equally to this paper.

centuries by *analytic proof* that became the major characteristic of the European mathematical tradition. At the beginning of 20th century, the foundational crisis led to the fundamental distinction between the *classical* and the *constructive* concepts of mathematical proof and the elaboration of different systems of mathematics (with different associated logical semantics) that make use of either the one or the other concept of *formal* proof. This distinction made proof dependent on the *admissible* axioms or rules of inference for the proof of mathematical theorems (Vandoulakis, Stefaneas, 2013a). Gödel's investigations in meta-mathematics, after the 20th century foundational crisis, shook down the established belief in the identification of proof with truth. During the subsequent years, mathematical logicians developed a great variety of formal representations of proofs in different formal languages. Nevertheless, many mathematicians were not willing to accept this kind of *formalistic* proof[2].

Joseph Goguen (1941-2006), proposed the concept of *proof-event*, designed to cover all particular exemplifications of proof: apodictic, dialectical, constructive, non-constructive proof, as well as proof steps and computer proofs.

> "Mathematicians talk of 'proofs' as real things. But the only things that can actually happen in the real world are proof-events, or provings, which are actual experiences, each occurring at a particular time and place, and involving particular people, who have particular skills as members of an appropriate mathematical community." …
>
> "A proof-event minimally involves a person having the relevant background and interest, and some mediating physical objects, such as spoken words, gestures, hand written formulae, 3D models, printed words, diagrams, or formulae (we exclude private, purely mental proof-events…). None of these mediating signs can be a "proof" in itself, because it must be interpreted in order to come alive as a proof-event; we will call them proof objects. Proof interpretation often requires constructing intermediate proof objects and/or clarifying or correcting existing proof objects. The minimal case of a single prover is perhaps the most common, but it is difficult to study, and moreover, groups of two or more provers discussing proofs are surprisingly common)" (Goguen, 2001).

The advantage of Goguen's definition is that proof is no longer understood as a static purely syntactic object, but as a *social process*, that takes place at a given location and time. It involves a public presentation of a purported solution of a particular problem before an appropriate mathematical community.

Thus, proof-events are not identical with mathematical facts, corresponding to mathematical truths, since a proof-event may concern an incomplete proof, a false proof or even a proofless exposition of ideas on a particular problem. Proof-events occur at specified places and times and, thereby are unrepeatable occurrences. They are temporally extended, so that they are deprived of full identity over time by their temporal parts. On the contrary, mathematical facts or states of affairs are considered as universals, i.e. timelessly existing or never existing necessarily; they are non-locatable and non-dateable.

On the other hand, the social group involved in a proof-event and other ordinary material things (handwritten formulae, 3D models, printed words, diagrams, or formulae, called *proof objects* by Goguen) have no temporal parts and are wholly present at every instant (time-slice) of a proof-

2 Mac Lane, for instance, emphasized, "Real proof is not simply a formalized document, but a sequence of ideas and insights" (Mac Lane, 1997).

event, since they have been introduced. Consequently, proof-events, mathematical facts and things (proof objects) are distinct types of entity.

Goguen's motivation for such a novel concept of proof stems from his research in automated theorem proving. In his words, the concept of proof-event

> "is more inclusive and less purely formal than that of traditional mathematical logic, in that it involves not only formal proof methods and formal proof steps, but also involves motivation for the proof and its major steps, background information, and the large grain structure of the proof, including conflict and other narrative devices. This notion of proof, which draws on the sociological study of the actual practice of proving, has been implemented in the Kumo[3] proof assistant and proof display system, … Success on this quest [i.e. to improve the understandability of proofs] could have a significant impact on mathematics education, given the impending pervasiveness of computers in schools, and the mounting frustration with current mathematical education practice. It could also make the current generation of more powerful theorem proving systems accessible to wider groups of users and new applications." (Goguen, 2001).

Thus, the introduction of the concept of proof-events was motivated by the need to provide a novel notion of proof that also embraces the act of proving and its major steps: the history of the proof, its relative background information, as well as its rhetoric and/or narrative features. This approach to proving was implemented for the first time in Goguen's Kumo proof assistant and its proof display system and it was based on a sociological study of the actual practice of proving. Despite the obvious impact that this approach can have upon mathematics education, the initial motivation was the creation of a powerful theorem proving system accessible to as wider as possible group of potential users. The Kumo system in its ideal design generates a website, called a *proofweb*, for each proof attempt that it executes. Using mathematical tools, such as hidden logics this website interleaves proof steps with explanatory material, according to conventions inspired by sociolinguistic analyses of narratives. In addition, in its expanded form it was designed to supply additional proof "components" such as interactive Java applets or "informal parts" of proofs.

Thus, the concept of proof-event was conceived, from the very outset, as more adequate notion for use in automated theorem proving and generally, in accomplishing problem solving or reasoning tasks, which is the heart of artificial general intelligence.

## 2. Mathematical Proving as Agents' Cooperative Activity

Proof-events presuppose at least two agents of two different types: a *prover*, which can be a human or a machine or a combination of them (hybrid proving), and an *interpreter*, who generally should be human (person or group of experts) or a machine (or group of machines) or a combination of them[4]. The prover and the interpreter may be separated by space and time (as, for instance, in the

3 Kumo is a Japanese word for spider.

4 In the case of constructive proofs, the correctness of a proof can be also checked by a computer program. However, such a program can find a gap in the formal working of a proof, but it is not designed for remedying it, i.e. for filling the gap. In addition, it is assumed that the proof checking software would have a core code liable to human hand checking.

In the case of Web-based proof-events, the agents commonly are more than two, because of the "massive" character of Web-based proving (Stefaneas, Vandoulakis, 2012; Stefaneas, Vandoulakis, Martínez and Foundalis, 2012, 2014).

case of asynchronous Web-based proving (Stefaneas, Vandoulakis, 2012)), but they are in *communication*. A human prover may experience an insight (intention) that something in mathematics is true and produce an item (using some semiotic code) to communicate his experience. This item may be not a proof, but an outline of a proof or even a conjecture. This initiates a proof-event. The end of the public communication of a purported proof can be considered as an ending point of a proof-event. The interpreter, who gets involved in this proof-event, perceives and reacts to it. In general, the item produced by a prover may lead to different communication outcomes (Goguen, 2001; Vandoulakis, Stefaneas, 2013a, 2013b).

Adopting the agent metaphor for studying proof-events raises both the visibility and abstraction level of interactions between agents, which are disregarded in the traditional mathematical-fact oriented approaches. An agent is an autonomous entity situated in an environment that might be a real *physical* one, like a material world inhabited by various kinds of things (objects), or a *virtual*, or a *simulated* one, when for instance human agents interact with physical tools and software entities or the Internet. An agent is equipped with past background knowledge and past learning experience. For example, an agent can be a coupling of a human with an expert system, a program that acts in a computational environment, a team of humans or combined human-agent teams, etc.

Agents enact different *roles*. The type of agent – prover or interpreter – determines its role with respect to a specified *problem*.[5] Enactment of a role by an agent means its engagement in *proving activity*, i.e. participation in a proof-event. The roles that agents may enact are interchangeable: an agent may enact the role of prover at one time and the role of interpreter at a different time of a proof-event[6].

Human agents act with *intention* and their activity is *goal*-oriented, depending on the type of agent. For example, the goal of a prover might be to solve a problem or to gain aesthetic pleasure from his proving activity and its outcome or both; the goal of an interpreter might be to understand the argumentation suggested by a prover, to check or disprove it. The goal can have sub-goals that can be associated with particular sub-problems or sub-tasks of the main problem. How a human agent decides to adopt a (proving) strategy, in order to meet a specified goal, by free choice or other processes, is another issue. To a human agent can be ascribed a *mental state*, like belief, intention, expectations, capabilities, etc. (Stefaneas, Vandoulakis, 2014). Different agents may have different capacities and resources; when their proving activity is directed towards the same-shared goal, this may result in a kind of increased collective capacity and enhanced effectiveness of the proving activity[7].

The capacity of a human to act as an agent is personal to that individual. This capacity is affected by the cognitive structure, which an agent has formed through his experiences, the views held by him and the community, eventual circumstances of the environment the agent is in, etc.

## 3. Layers of Communicative Interaction between Agents

Since agents are social entities, they are able to interact with other human or manmade agents, in order to achieve a goal (i.e. a proof of a problem) or help others to do that. The layers of interaction between (minimally) two agents are:

1. Communication

5 In the case of Web-based proof-events, the agents can play different roles at different times (Stefaneas, Vandoulakis 2012).

6 This is typical in Web-based proving (Stefaneas, Vandoulakis, 2012).

7 This collective agency capacity is characteristic to Web proof-events (Stefaneas, Vandoulakis, 2012).

2. Understanding
3. Interpretation
4. Validation

Each layer presupposes its preceding one, but not vice versa. Each higher layer adds more features.

**Communication**. The environment provides the surrounding conditions for agents to exist and communicate and serves as a *means of communication* for agents. The means of communication include written text (manuscripts, printed or electronic texts, letters, shorthand notes, etc.) in (ordinary or formal) language or any other semiotic code of communication (signs, formulae etc.). The environment provides also conditions for oral communication (lectures, etc.), visual (non-verbal) communication (diagrams, movies, Java applets, etc.), as well as communication through practices.

The communication process takes place between a prover and an interpreter (or, at least, an intended interpreter) which both participate in a proof-event, although they may act in different geographical locations, be surrounded by different environments at different times and belong to different mathematical cultures. However, they must share a common *interpersonal space*, for communication to be possible. There are different ways to communicate mathematical ideas or proof insights and different proofs can be devised for some problem by different mathematicians, belonging to different cultures and times. This is a sign that the initial intentions and the items that are proposed as proofs of these intentions have *inter-subjective* character.

The prover conveys a mental construction, encoded in some semiotic *code* (in a *text*, in the semiotic sense), whereas the (potential) interpreter must perceive this "text" as a possible proof, so to respond and undertake the task of decoding it. The prover expects that the interpreter will be persuaded that the transmitted construction is actually a proof. His confidence about that stems from the prover's personal firm belief that he was not betrayed by his own intuition. This induces an ethical aspect in the relation of the prover with the interpreter and before the academic community, in general (Bazhanov, 2011).

The "text" usually consists of signs of the natural language, signs of some mathematical language, possibly graphs, charts, abbreviations, etc.; it has the form of ***narrative*** structure, organized in a complex hierarchical order[8]. Moreover, the "text" is formulated by the prover in some specific ***style***, incorporating various communication functions. The style can be personal for a prover or for the school he belongs (for instance, the well-known Bourbaki style of mathematical exposition) or for a whole tradition (for instance, the Euclidean style of the *Elements*, or the Neo-Pythagorean style of Nicomachus' *Arithmetic* (Vandoulakis, 1998, 2009, 2010). It may be also mimicry of the style of a renowned authority[9]. The style is a ***meta-code*** that determines the *selection* of a particular code and the *combination* of blending principles to produce the "text" by the prover (Stefaneas, Vandoulakis, 2014).

**Understanding**. Understanding a mathematical "text" (i.e. a suggested item that is supposed to be a proof) does not come simply from reading the "text". The meaning that the prover may ascribe to the "text" (the *intended meaning*) is generally different from the *perceived meaning* that the interpreter may ascribe to the same "text". Moreover, the prover and the interpreter may follow *different kinds of ("local") logic* in their reasoning. Understanding is achieved when the (structure of) meanings perceived by the interpreter corresponds to the intended (structure of) meanings of the prover, i.e. when a mapping, called ***semiotic morphism*** (or "translation" or "representation")

8 For further details, see (Stefaneas, Vandoulakis, 2014).

9 This is characteristic, for instance for the *Principles of Mathematical Analysis* (McGraw-Hill, 1953) by Walter Rudin (1921-2010), who strives to mimic Bourbaki's style.

(Goguen, 1999a, 256; 2003), can be established from the semiotic space of the prover into the semiotic space of the interpreter. Thus, understanding is attained at a higher level than the "local" logics of the agents.

A ***semiotic space*** is an algebraic many-sorted structure – organized in layers - with an arbitrary number of domains; the sorts play the role of names that signify objects for the different domains. Signs of a certain sort are represented by terms of that sort; they may be whole words, sentences or paragraphs in natural language, as well as complex entities of arbitrary nature (figures, graphs, etc.) that are treated as single objects (Goguen, 1999a, 2003; Stefaneas, Vandoulakis, 2014). A semiotic space serves as the "context" of the signs. It may include conventional meanings of the signs, information on their importance and use, meanings rooted in a stable (individual or disciplinary/academic) tradition, etc., which are important for the determination of the meaning of the signs and their possible communicational functions. Signs and semiotic space constitute the ***code*** in which mathematical information is encoded by a prover. An interpreter, who shares a code, or logic different from that of the prover, may fail or have difficulties in understanding the prover's code.

Goguen's theory of semiotic spaces is grounded on Gilles Fauconnier and Mark Turner's theory of *conceptual spaces* (Fauconnier, Turner 2008), according to which cognition takes place by mind's subconscious *integration* or *blending* of various conceptual spaces, consisting of elements and relation instances between them, and resulting in the creation of a new *blended* space out of parts of the initial spaces. However, Goguen substitutes the conceptual spaces of cognitive linguistics with his own concept of semiotic spaces, because

> "Whereas conceptual spaces are good for concepts, they are inadequate for structure" (Goguen, Harell 2004a, 2010, 299).
>
> "Whereas conceptual spaces are good for studying meaning in natural language, they are not adequate for user interface design and other applications where structure is important" (Goguen 2003).

Thus, besides elements and relations, Goguen requires from a space to have multi-argument constructors, sorts, levels, priorities, or axioms. Accordingly, conceptual blending of conceptual spaces is substituted by *structural blending* or *structural integration* of semiotic spaces, which uses algebraic semiotics to describe complex structures of signs and blends of such structures. This enables developing computational accounts of blending, which have been developed in algebraic theory and algebraic semiotics. Furthermore, semiotic morphisms are not just mappings between space entities, but mappings between structures comprising entities with internal states. Thus, in structural blending, the emergence of cross-space mappings becomes more complex, because more than one blend is possible for a given system of spaces and morphisms.

In proving we need to take also into account the structure of the proof, not just the relation of concepts upon which a proof might rely. There are at least two perspectives that one might take into account in proving. The perspective of the prover, whose function is to "construct" a proof, and the perspective of the interpreter, whose function is to understand the structure of a purported proof, understand the principles of its "construction" and, in this way, to get engaged in the process of testing and validating it. Although understanding of a "text" by an interpreter is a prerequisite to its interpretation, this does not guarantee yet the truth of the proof.

**Interpretation**. This is the determination of the definition or meaning of signs, which are fixed by the language or communication code used for the presentation or transmission of a proof or what is thought of to be a proof. The communication code contains symbols and rules for the combination (syntax), interpretation (semantics) and application (pragmatics) of those symbols that have been agreed upon to use or have to be decoded.

Interpretation is an active process, during which the interpreter may amend the initial proof by adding new concepts (definitions) by filling possible gaps in the proof, etc. In some sense, interpretation is a reconstruction of meaning or conscious reproduction of the information content conveyed by the "text". During this process, the interpreter may choose even a new, different code to express the meaning of the prover's "text". However, he does not usually transfer the stylistic characteristics of the source "text", but focuses on the correct explication and reformulation of its meaning. The meta-code specifics serve communicative purposes and may facilitate (or hinder) understanding the meaning of the prover's "text", but are not necessarily preserved during interpretation. Interpretation is generally articulated in a blend of styles contemporary to the interpreter, including possibly also elements of the style of the prover.

Interpretation by means of a new code may also enhance understanding and contribute to the validation of the outcome. This seems essential in the case of computer proofs, where the prover is non-human agent. For instance, William McCune proved Herbert Ellis Robbins' (1915-2001) conjecture, that is, the thesis that all Robbins algebras are Boolean (McCune 1997) in 1996, using the so-called *Equational Prover*, that is an automated theorem proving program for first-order equational logic. Before the computer-generated proof, many mathematicians had attempted to give a proof, beginning with Edward Vermilye Huntington (1874-1952) (Huntington 1933a, 1933b), Alfred Tarski (1901-1983) (Henkin, Monk and Tarski 1971), S. Winker (Winker, 1990, 1992) and others, but in vain. Further, McCune's proof was successfully verified by another automated theorem-prover for first-order and equational logic, called "Otter". Nevertheless, the proof remained unintelligible by a human agent. The form of reasoning used by the Equational Prover was beyond human understanding and interpretation. The computer proof became acceptable from the mathematical community, only when Louis H. Kauffman "translated", i.e. interpreted the computer proof into a new diagrammatic language of nested box algebra (Kauffman, 1990, 2001), that is, when he used a new, more appropriate and intelligible code for the representation of the proof.

**Validation**. A proving is complete when the agents involved in a proof-event conclude that they have understood the proof and agree that a proof has actually been given, i.e. that the proof is a fact. However, there are cases of computer-generated proofs that the validation of the proof by humans is not practically possible, since no human or group of humans is capable to check a huge number of proof steps[10]. What can be considered as validation in such a case is the validation of the correctness of the theorem-prover itself (as a program). Validation of the program can guarantee that all possible proofs generated by this software tool have been "validated". One way or the other, either by human or by automated means, the final output of the validation marks the termination of the proof-event at this particular time. The truth of the proof is ultimately declared by the relevant mathematical community, which is recognized as competent to check the proof. Accordingly, the mathematical community is the ultimate (collective) truth-maker of a purported proof. Thus, validation is a social process that involves the collective mind of the mathematical community. The case of a "proof" that is understood by only one agent is not acceptable, because it contradicts the intersubjective nature of mathematical proof.

The process of validation is always finite in time: the mathematical community within a finite (although, possibly very long) time interval will conclude on a proof, either in positive or in

10 Examples of such proofs are, for instance the famous four-color theorem or Herbert Ellis Robbins' (1915-2001) conjecture, that is, the thesis that all Robbins algebras are Boolean (see (Vandoulakis, Stefaneas 2013a) for more details).

negative. The validation process may involve the outcomes of other proof-events, crosschecking, applications to similar problems, etc. Once the outcome of a proof-event is confirmed, it is further considered irrefutable and reliable by the appropriate group of the academic community and is integrated into the mathematical heritage.

## 4. The Temporal Extension of Mathematical Proof-events

Each proof-event has temporal extension and, thereby a history: it has a starting point i.e. a point that the proof-event is initiated by the statement of a problem or idea or conjecture, and a termination point, i.e. a point that the proof-event is considered ultimately completed and validated. Thus, proof-events have temporal extension. A proof-event that has duration can be decomposed into an instantaneous proof-event that starts it, followed by a state of continuous change, followed by an instantaneous proof-event that ends it.

What is posed to be proved, i.e. the initial problem or idea, emerges often out of history, during the unfolding of *sequences of proof-events*. Thus, the initial intention or insight of a proof bears a historical meaning that can also mark the significance of a proof and affect its historical impact. For instance, the announcement of the famous Hilbert's problems[11] is a ground-breaking proof-event that took place on 8 August 1900 in the Sorbonne, at the Paris Conference of the International Congress of Mathematicians. The problems Hilbert posed before the international community of the mathematicians varied in nature and precision of formulation. They had emerged in the course of unfolding of different sequences of proof-events in a variety of areas (foundations of mathematics, algebra, number theory, geometry, topology, algebraic geometry, Lie groups, real and complex analysis, differential equations, mathematical physics, probability theory and calculus of variations). All the twenty-three problems announced were unsolved at that time – they were simply conjectures. Yet, they mark the starting point of new sequences of proof-events. Sixteen problems are solved today, i.e. the sequences of proof-events they initiated are completed. Two of them were ill stated as mathematical problems, so that they could not be checked and validated or refuted and thereby they cannot be considered as proof-events at all. Three of them are partially solved, i.e. the sequences of proof-events they initiated are incomplete, but have completed sub-sequences of proof-events (representing solutions for particular cases). Two of them remain unsolved today, that is the sequences of proof-events they initiated is still incomplete.

Moreover, the semiotic code chosen by the prover to communicate his intention or idea has also historical nature. One code can be more suitable for the communication of an intention, while another can be proved less suitable. In the course of a sequence of proof-events, the initial code used for the formulation of a problem may be abandoned and replaced by another code, more suitable for proving specific proof parts or for the final proof. For instance, Fermat's conjecture that no three positive integers $a$, $b$, and $c$ can satisfy the equation $a^n + b^n = c^n$, for any integer $n$ greater than two, that marks the starting point of a sequence of proof-events, was formulated in the language (code) of Diophantine analysis. However, its solution needs a more appropriate and powerful language (code) to be expressed: the language of algebraic geometry. During the 358 years that this sequence of proof-events was evolving, the rhetoric of the proof-events concerning this problem underwent changes several times and every time the problem was "translated" into the new language adopted at that time (Aczel, 1997; Kleiner, 2000; Singh, 1998).

---

11 Hilbert's lecture appeared in the *Göttinger Nachrichten*, 1900, pp. 253-297, and in the *Archiv der Mathematik und Physik*, 3d ser., vol. 1 (1901), pp. 44-63 and 213-237, See also (Demidov, 1966, 2001).

Proof-events that occur at specified places and times and involve the same group are unrepeatable occurrences, and in this sense, are unique. However, it may happen that two proof-events have the same starting point, in the sense, that they start from the same or logically equivalent problems and the same termination point, i.e. they are completed by the same or logically equivalent validated solutions, although the concepts and methods used to achieve these solutions may differ substantially. These proof-events express *independent outputs*, which may take place in different places, but in the same time or almost the same time (*independent synchronous* proof-events) or in different times (*independent asynchronous* proof-events), when, for example, a prover re-discovers a mathematical fact, without being aware that this fact has been already established by another prover in the past. The latter case raises the vital question of *historical priority* of the proof, which is decided again by the relevant mathematical community on the ground of the comparison of the proving outcomes.

Independent outputs of proof-events occur very often in history of mathematics. We mention here: the discovery of the non-Euclidean geometry by Nikolai I. Lobachevsky (1792-1856) and János Bolyai (1802-1860); the method of coordinates by René Descartes (1596-1650) and Pierre de Fermat (1601 or 1607-1665); the invention of logarithms by John Napier (1550-1617) and Jost Bürgi (1552-1632); the theory of elliptic functions by Niels Henrik Abel (1802-1829) and Carl Gustav Jacobi (1804-1851); the discovery of the topological theory of dimension by Pavel S. Urysohn (1898- 1924) and Karl Menger (1902-1985), that was commemorated in the term *Menger-Urysohn dimension*. The pairs of outputs listed above are independent outcomes of distinct sequences of proof-events that were evolving in different places and involved different provers. In this sense, each proof-event of the pair is unique. They can be considered identical only in the sense that the outcomes of the corresponding sequences of proof-events can be proved logically equivalent.

Therefore, two proof-events that have the same "initial" (i.e. the same problem or logically equivalent problems) and "terminal" points (i.e. the same outcome or logically equivalent outcomes) can be considered as *equivalent*.

## 5. On the Problem of Change in Mathematical Proving

The concept of *proof-event*, instead of *mathematical fact*, is adequate to study the concept of change in mathematical knowledge. It was Thomas S. Kuhn's concept of scientific revolution that awakened the interest in the concept of *change* in scientific knowledge. The theory of proof-events provides a logical framework to study change in mathematical knowledge, because it incorporates the intuitive idea that any change (including change in mathematics) must be due to some cause.

First, *change* can be defined as an ordered pair of proof-events $\langle e_1, e_2 \rangle$ that happen in two (generally, distinct) semiotic spaces $S_1, S_2$. Further, the concept of *trajectory* expresses the advancement of the state of a proof-event, caused by some action (e.g., solving activity)[12], through space as a function of time. Then, the question of change in mathematical knowledge can be examined in terms of the concept of continuity or discontinuity of a trajectory joining two distinct proof-events in the corresponding semiotic spaces.

Intuitively speaking, continuous change can be understood as "smooth" advancement of the state of a proof-event. During continuous change, validated outcomes of proof-events that hold in

12 Actions can be causes of which events are effects (Davidson, 1967).

time $t_1$ in a semiotic space $S_1$, hold also in subsequent time $t_2$ in a semiotic space $S_2$ (but not vice versa). On the contrary, discontinuous change represents an abrupt change or jump. Outcomes of proof-events that hold in time $t_1$ in a semiotic space $S_1$, may not hold in subsequent time $t_2$ in a semiotic space $S_2$. This does not mean, however, that the initial outcomes of a proof-event cease to hold in the original semiotic space $S_1$. The resulting semiotic space $S_2$ co-exists on a par with semiotic space $S_1$. Such changes are caused by radical changes, for instance in the system of axioms adopted for the solution of a problem or in a transformation of semantic assumptions, which may affect radically the structure of the underlying semiotic space, giving rise to a bifurcation of semiotic spaces.

In other words, continuous change is a truth-preserving transformation with respect to semiotic spaces, whereas in discontinuous change, truth is not necessarily preserved in the emerging semiotic space or is preserved for a modified analogue of the initial problem. For instance, the Heine-Borel theorem holds true in the world of classical mathematics, but in the world of intuitionistic mathematics holds true a modified analogue in terms of the intuitionistic concept of "pointspecies", whereas in the world of constructive mathematics of Markov's school this theorem does not hold true (Vandoulakis, 2015, 151).

Continuous change may involve significant transformations in a sequence of proof-events: conceptual transformations, introduction of new concepts or a new code, devise of innovative approaches, application of new methods, etc. In such cases, there is always a trajectory that joins any point (proof-event) of the sequence before the change with a point (proof-event) after the change (but not vice versa), in spite of the extent of transformations that took place.

On the contrary, discontinuous change involves radical transformation in axiomatics or semantics and, thereby in the associated underlying ontology: different kinds of mathematical entities are considered as existing before and after the point of discontinuity. In this case, there is no trajectory that may join *any* two points (proof-events). Proof-events before and after a discontinuous change belong to different mathematical systems, or "worlds" or "paradigms" in Kuhn's terminology; they might be "incommensurable". For instance, a non-constructive proof of existence, i.e. a proof that involves *reductio ad absurdum*, may be understood by a classical mathematician, but it is not "understandable" by a constructivist (Vandoulakis, 2015, 145-151). The fact that a theorem does not hold true in some version of constructive mathematics that was developed at a later time than classical mathematics does not imply, however, that the truth of that theorem has been disproved or rejected in classical mathematics. The phraseology that the intuitionists use when they talk about "rejection" of a classical theorem is grounded on their belief that intuitionistic mathematics is the only acceptable one.

We clarify these concepts with examples from the history of mathematics. A notable figure, who marks a turning point in the development of algebra, is François Viète. In his *In artem analyticem isagoge* (1591) he exposes the foundations of a new science, designed to "leave no problem unsolved" (*nullum non problema solvere*) (Klein, 1968, 344). The fundamental transformations he introduced concern (Bashmakova, Smirnova, 2000):

a) The concepts: He divided algebra into two parts: the first part, called *logistica speciosa*, concerns general magnitudes, whereas the second (*logistica numerosa*), concerns numbers. Before Viète, the mathematicians were confined to numbers only.
b) The code: before Viète, literal notation was restricted to the unknown and its powers (introduced by Diophantus and the mathematicians of the 15-16$^{th}$ centuries); he also introduces literal notation for parameters.

Under these transformations, the (validated) outcomes of proof-events, established earlier (e.g. by Arabic mathematicians) remain valid. No outcome was dropped or invalidated.

However, this is not the case, with the appearance of non-Euclidean geometries, or non-classical mathematics (i.e. intuitionistic mathematics and the various versions of constructive mathematics), or non-standard (non-Archimedean) analysis. Validated outcomes of proof-events in Euclidean geometry, classical mathematics or (standard) analysis may not hold in their "non-standard" counterparts. In particular, the theorems and proofs of Euclidean geometry that depend upon the axiom of parallelism are not preserved in non-Euclidean geometries. The theorems and proofs of classical mathematics that depend upon the principle of excluded middle are not preserved in the varieties of constructive mathematics. Theorems and proofs that depend upon the Archimedean axiom are not preserved also in non-standard analysis. Therefore, the appearance of non-standard mathematical systems marks an essential point of discontinuity.

Consequently, discontinuous change is related with possible *proliferation of mathematical systems* or *worlds*. These systems or worlds are co-existing "paradigms" (if we use Kuhn's terminology), in contrast to Kuhn's theory, where a paradigm shift invalidates the earlier paradigm. The feature of proliferation of mathematical worlds characterize discontinuous change in mathematics, but not necessarily in the physical sciences.

## 6. Towards a logical representation of mathematical proving

We outlined above an informal theory of mathematical proving, based not on the concepts on mathematical fact and truth, but on the concept of proof-event, i.e. proof-process, in order to capture essential aspects of the process of mathematical problem-solving activity that are not considered within traditional philosophies of mathematics, but are important for Artificial Intelligence, which focuses on problem-solving and reasoning procedures. This theory cannot possibly be represented by means of a unifying model, because of the variety of its aspects. For instance, the communicative aspects of a mathematical text, such as the mathematical style, need specific models. In this paper, we confine ourselves to represent certain features of the temporal extension of mathematical proof-events in terms of the calculus of events. The latter was first formalized by Robert Kowalski and Marek Sergot (1986) and was further extended by Murray Shanahan and Rob Miller (1999).

Using the language of event calculus, we can speak about proof-events and their sequences. The calculus of proof-events requires a many-sorted predicate logic with equality, with sorts for

- Individual physical objects (humans, chairs, tables, etc.).
- Real numbers, to represent (chronological) time and variable quantities.
- Time-dependent properties, such as *states* and *activities*.
- Time-independent propositions, called *problems* (specified by certain (time-dependent) *conditions*)[13].
- Variable quantities.
- *Types of proof-events*, whose instantiations mark the beginning and end of time-dependent properties.

The fundamental concepts are the *proof-events* and the *fluents*.

13 Following A.N. Kolmogorov (1932), we do not define what a problem is. Certainly, the way we understand problems is far from unequivocally definite and general. Thus, a problem may be the starting point of different sequences of proof-events. Nevertheless, a problem remains fixed, unless it is terminated. The conditions of the problem may change, when it is realized that they are inadequate for the solution of the given problem.

**Proof-events** *e* take place in space and time (*proving instances/ occurrences*); they refer to a fixed problem (proposition), specified by certain *conditions* (predicates). A proof-event *e* has the following internal structure:

$$e \ll \left\langle present(Intention, Problem), t \right\rangle,$$

which means that an *intention* (insight or idea or proof sketch, or mathematical argument, etc.) is linguistically articulated for a (time-independent) *problem* (formulated in the form of a mathematical proposition, specified by certain *conditions*) at time *t*, which conventionally denotes the time that the communication (*presentation*) has been completed[14]. In this case, we say that the presented output (semiotic "text") is an *exemplification* or an *instance* of a proof-event with respect to the particular fixed problem.

**Fluents** *f* are sequences of proof-events (proving instances) $\{e_n\}_{n=1,2,3,}$ evolving in time that refer to a fixed problem. A fluent is a function that may be interpreted in a model as a set of time points $\{t_n\}_{n=1,2,3,}$, conventionally denoting the time when the communication output is available. Hence, fluents, like proof-events, have "initial" and "terminal" points, i.e. they are extended spatially and temporally.

Thus, the underlying *ontology* (the types of entities over which quantification is admissible) contains (types of) *proof-events*, *fluents* and *time points*.

The *value of a proof-event* (outcome of a proving instance) expresses the subjective conviction of the community of agents participating in the proof-event in the truth of the outcome; it can be estimated as the subjective (Bayesian) probability of the community participating in the proof-event in the truth of the proving outcome. Frequentist probability is not applicable in this case, because communication of a purported proof is neither an experiment that is repeated under the same conditions, nor a hypothesis that has to be tested. On the contrary, Bayesian probability is suitable because it represents a state of knowledge or a state of belief. A purported proof is viewed by the relevant community as a hypothesis (whose truth or falsity is uncertain until its validation) to which is assigned a probability.

The *value of a fluent* is subject to change over time, depending on the value of the individual proof-events; it is equal to the value of the proof-event $e_i$ at time $t_i$.

The basic temporal predicates for modelling continuous change are:

$Happens(e,t)$, which means that a proof-event *e* occurs at time *t*.

$Initiates(e, f, t)$, which means that if a proof-event *e* occurs at time *t*, then the fluent *f* (sequence of proof-events) remains active after *t*, which is the starting time-point of a sequence of proof-events. This does not mean that the proving outcome is (recognized as) valid or true at time *t*.

$Terminates(e, f, t)$, which means that if a proof-event *e* occurs at time *t*, then the fluent *f* (sequence of proof-events) will be *inactive* after *t*, which is the termination (time point) of the sequence of proof-events. The termination of a sequence of proof-events may be caused by the proof of falsity of the problem (failure under the specified conditions), or the undecidability of the problem (failure to construct an algorithm that leads always to a correct yes-or-no answer).

14 Following Kowalski, we assume that "the event calculus is actually neutral with respect to whether events are instantaneous or have duration" (Kowalski 1992, 122). In some cases, the starting time-point of a proof-event is difficult to be identified or agreed, whereas the termination time-point is associated with the availability of the output of communication. The philosophical questions underpinning the choice between the options "time as 'flow' or duration" and "time as 'instants' or time-points" is beyond the scope of the present paper.

Oblivion of the problem by the mathematical community cannot be considered as termination point for a sequence of proof-events.

Two proof-events (fluents, respectively) are called *(logically) equivalent* if and only if they have the same "initial" (refer to logically equivalent problems) and "terminal" points (logically equivalent outcomes).

Temporal binary predicates can be defined over the set of proof-events to express their possible relative order, i.e. such concepts as "precedes", "follows", "begins before", "ends before", etc. in terms of time order. Proof-events may occur *concurrently*, whenever $Happens(e_1,t_1)$ and $Happens(e_2,t_2)$, where $e_1 \neq e_2$ and $t_1 = t_2$. They may be *overlapping* at *t*, whenever $Happens(e_1,t_1)$ and $Happens(e_2,t_2)$, where $e_1 \neq e_2$ and $\exists t,t',t''((t_1 = t' + t) \wedge (t_2 = t'' + t)$.

The aim of the use the language of event calculus in describing proof-events is to model the evolution of the sequences of proof-events in terms of fluents, defining the value of each fluent after an arbitrary proof-event (proving instance) has been performed. Thus, the common principles or axioms of the calculus of events that relate the above predicates together, can serve to model the evolution of a fluent in terms of the value of each fluent after the occurrence of an arbitrary proof-event.[15]

A fluent began to be "active" or "perspective" after time *t*, if and only if it was active in the past, and has not become inactive in the meantime, i.e.

$ActiveAt(f,t)\ \text{É}\ \ Happens(e,t) \wedge Initiates(e,f,t)$.

If there is a terminating proof-event between $t_1$ and $t_2$, this is expressed by the predicate $Clipped(t_1,f,t_2)$, i.e.

$Clipped(t_1,f,t_2)\ \text{É}\ \ \exists e,t\left[Happens(e,t) \wedge (t_1 \leq t < t_2) \wedge Terminates(e,f,t)\right]$.

If a proof-event *e* has taken place at time $t_1$, prior to $t_2$ that has initiated the fluent *f*, which has not been terminated at a time between $t_1$ and $t_2$, then the fluent *f* (sequence of proof-events) remains active at time $t_2$:

$Happens(e,t_1) \wedge Initiates(e,f,t_1) \wedge (t_1 < t_2) \wedge \neg Clipped(t_1,f,t_2) \rightarrow ActiveAt(f,t_2)$.

Continuous change requires the predicate for trajectory: $Trajectory(f_1,t_1,f_2,t_2)$ which means that if the fluent (sequence of proof-events) $f_1$ is active during the interval $(t_1,t_2)$, then the fluent $f_2$ will be active at time $t_2$.

In addition to the above general principles, it is necessary to introduce axioms specific to the mathematical domain under consideration. These axioms would define which proof-events could be proved to be equivalent, which ones are known to be true or false (validated) and, thereby make the corresponding fluents true or false, respectively.

## 7. On The Semantics of Agents' Proving

We have argued (Vandoulakis, Stefaneas 2014) that that the logic of agents participating in a proof-event can be expressed in terms of Andrey N. Kolmogorov's (1903–1987) *calculus of problems* (Kolmogorov, 1932), initially conceived as interpretation of Luitzen Egbertus Jan Brouwer's (1881–1966) intuitionistic logic of propositions, anticipating Arend Heyting's (1898–1980) semantics for intuitionistic logic (Heyting 1956).

15 Various alternative axiomatizations have been suggested by Miller and Shanahan (1999).

- Proving of the problem (intuition) "*A* & *B*" means proving of the problem (intuition) *A* and proving of the problem (intuition) *B*.
- Proving of the problem (intuition) "*A* or *B*" means proving of the problem (intuition) *A* or proving of the problem (intuition) *B*.
- Proving of the problem (intuition) "*A* implies *B*" means "reduction" of the problem (intuition) *B* to the problem (intuition) *A*.
- Proving of the problem (intuition) "not *A*" means that the assumption of a solution of the problem (intuition) *A* implies an absurdity.
- Proving of problem (intuition) "for all $x, A(x)$" means proving intuition *A* for any (arbitrary) object from the domain of *x*.
- Proving of problem (intuition) "there exists an $x, A(x)$" means proving problem (intuition) *A* for an indicated (given) object *c* from the domain of *x*.

In this way, Kolmogorov interpreted intuitionistic logic of propositions as logic of problem solving. Problems cannot be asserted; they cannot be, like propositions, true or false. Kolmogorov explains his motivation in a letter to Heyting dated 12-X-[19]31 (Kolmogorov 1988):

> "Each 'proposition' in your framework belongs, in my view, to one of two sorts:
>
> (a) *p* expresses hope that in prescribed circumstances, a certain experiment will always produce a specified result. …
> (b) *p* expresses the intention to find a construction. …
>
> I prefer to keep the name *proposition* (Aussage) only for propositions of type (a) and to call "propositions" of type (b) simply *problems* (Aufgaben).

Although Kolmogorov conjectured that his calculus of problems coincides with intuitionistic propositional logic, Heyting originally admitted that Kolmogorov's interpretation goes beyond the intuitionistic premises (Heyting 1955, 17)[16].

The semantics of provings in terms of Kolmogorov's calculus of problems is parallel to the concept of proof as "fulfillment of intentions", in the sense of Husserl's theory of intentionality, suggested by Heyting (1931) or the notion of proof as "realizations of expectations" suggested by the contemporary philosopher of mathematics Richard L. Tieszen (1989, 1992, 2000, 2005). In all these approaches, proof is understood not as completed abstract object, but as a sequence of acts that could be conducted in time. In Tieszen's words

> "To say that proof is a "process" in which an intention comes to be fulfilled is to say that it is a process of carrying out a sequence of acts in time in which we come to see an object or in which other determinations relevant to the given intention are made" (Tieszen, 1992, 25).

Thus, Kolmogorov's calculus of problems is suitable for the interpretation of agents' proving activity (proof-events), because it is not based on the notion of 'truth', but relies on the concepts of 'problem' and 'solution to a problem', i.e. the 'process' or construction of proof (which is understood as 'mental' construction, by Brouwer). Likewise, the truth of a purported proof in a proof-event is not given beforehand; instead, proof-events are defined in terms of the concepts of 'problem' and 'purported solution to a problem' ('intention'). Kolmogorov's calculus of problems

16 Later Heyting came to regard Kolmogorov's calculus of problems as essentially the same with his own interpretation of intuitionistic logic (Heyting 1958).

provides the desired semantics for the calculus of proof-events, i.e. of proofs as processes. This is a 'loose' semantics, in the sense that Kolmogorov's calculus of problems serves as informal explanation of intuitionistic logic and itself requires formalization[17]. Moreover, Kolmogorov's interpretation

> "is very close to programming. "*a* is a method [of solving the problem (doing the task) *A*]" can be read as "*a* is a program … which meets the specification *A*". In Kolmogorov's interpretation, the word problem refers to something to be done and the word program to how to do it." [Martin-Löf 1984, 4].

Consequently, not only the calculus of proof-events, but also Kolmogorov's semantics in terms of calculus of problems are adequate formalization tools that enable developing computational accounts of the process of proving. Unfortunately, Kumo had also limited impact on automated theorem proving

## 8. Intended Interpretations

As we have already mentioned, the concept of proof-event was motivated by Goguen's research in automated theorem proving, as implemented in his Tatami distributed cooperative proving project that consists of the Kumo proof assistant and its proof display system (Goguen 1999b). The Kumo system generates a website, called a *proofweb*, which is a data structure for each proof attempt that it executes. A proofweb integrates browsing, execution, animation, and informal explanation with formal proofs. The proofwebs are essentially instances of proof-events, insofar as they are actually communication outputs of proof attempts.

Another project of distributed cooperative proving was initiated by Timothy Gowers [*G*], a Fields Medal-winner Cambridge mathematician, in 2009. He called on the community in his blog to find a new, more intelligible, solution of a special case of the density Hales-Jewett theorem [DHJ] (Hales and Jewett 1963). This marks the beginning of a proof-event, i.e. the system starts from the state $\langle G, DHJ \rangle$. Each agent $A_i$, who joined the system, had to use the comment function of Gowers's' blog to communicate insights, ideas, approaches, pieces of proof, etc. (whenever acted as prover), or to comment, correct, or reject ideas proposed by other agents (whenever acted as interpreter). Each attempt has the features of a brainstorming session and represents by itself a proof-event in a sequence of proof-events. The evolution of the sequence in time is represented in the "history" kept by the medium (the blog)[18]. The attempts (proof-events) were developed in time along two main sequences of proof-events in the respective blogs of Gowers and Terence Tao, another winner of the Fields Medal. Both sequences produced outputs that were finally evaluated as actual proofs of the problem and were published under the pseudonym "Polymath" (2009, 2010a, 2010b), which denotes a collective author[19].

The Polymath project was the first real experiment of collective Web-based proving carried out by agents of varied knowledge background and expertise skills, who worked as a goal-directed system. A blog was used to create an interest-based community of agents, whose exchange and

---

17 Kleene realizability (Kleene 1945) and Medvedev's finite problems (Medvedev 1962) are considered as such formalizations.
18 See the Polymath project's timeline: http://michaelnielsen.org/polymath1/index.php?title=Timeline.
19 Because of its collective nature, the final outcome of a Web-based proof-event cannot be credited to its initiator or the supervising agent.

cross-fertilization of ideas amplified collective creative thinking that led to a fast solution of the problem.[20]

Proceeding from an analysis of the aforementioned instances of Web-based proof-events and the role that collaboration plays in creative thinking, we invented a mental experiment for the study of collective problem solving, discovery and creativity, using also, for the first time, ideas from cognitive architectures [Stefaneas et al 2015]. In this imaginary model, a proof-event is initiated by the posting by an agent $A$ of a single task: to prove the Pythagorean Theorem ($PT$). Thus, the system starts from the state $\langle A, PT \rangle$, where $A$ is the supervisor of the task $PT$. The supervising agent can define conditions, denoted as $PT_i$ $(i = 1,2,3,4)$ that a proving of $PT$ is required to fulfil. An agent $A_i$, interested to undertake the role of a prover for one of the $PT_i$, is admitted to join the system. Thereby, the system switches to a new state with four agents $\langle A_1, PT_1 \rangle, \langle A_2, PT_2 \rangle, \langle A_3, PT_3 \rangle, \langle A_{41}, PT_4 \rangle$, supervised by the initial agent $A$. In the course of proving, new subtasks are posed, which generate subsequences of proof-events, aiming at fulfilling particular tasks. These subtasks might appear out of communication disturbances (certain points in a suggested purported proof can be evaluated as unintelligible or unconvincing) or stylistic preferences (use of a particular code, etc.). Thus, the proving activity of the agents depends on their knowledge background, creative abilities, and proof-stylistic preferences – what could be defined as "agent's *profile*". The agents at the highest level of the hierarchy generally possess a higher level of expertise.

A system like that described above keeps track of the whole "history", evolving in time, of the collective, non-linear process of discovery of a proof, including the procedures of checking, acceptance or rejection by individual agents or the community of the agents.

## 9. Conclusions

In this paper, we exposed the essentials of a logical model for the practice of mathematical proving, that takes into account certain aspects that are important in Artificial Intelligence and allow the development of computational approaches. Proceeding from the concept of *proof-event* or *proving*, introduced by Goguen in connection with the Kumo project, as problem-centered spatio-temporal processes, where the agents enact different *roles* (of the *prover* and/or the *interpreter*), we examined the levels of communicative interaction among agents. These interactions form an ascending hierarchy: communication, understanding, interpretation, validation.

Further, we described certain essential aspects of the spatio-temporal nature of proof-events, i.e. that proof-events have *history* and form *sequences of proof-events* evolving in time, which are required to be captured by our proposed model. We also described the problem of change in mathematical proving in terms of proof-events. This topic is important, because radical transformations of the underlying assumptions regarding a problem might take place in the course of a sequence of proof-events that may lead not only to the "enrichment" of the underlying semiotic space, but also to the creation of a new independent semiotic space, within which the proof-search procedure could deliver a valid output.

Our logical representation of proof-events is modeled upon Kowalski's calculus of events, which provides the necessary conceptual arsenal to represent proof-events, sequences of proof-

20 See (Stefaneas, Vandoulakis 2012) for a more detailed account of the Kumo and the Polymath projects as Web-based proof-events.

events (fluents), and other relevant temporal predicates. The semantics for proof-events can be provided by Kolmogorov's calculus of problems, which is essentially the first-ever stated logic of problems, conceived as informal interpretation of Brouwer's intuitionistic logic of propositions. In contrast to the traditional concept of *proposition* as bearer of truth-value, Kolmogorov's concept of *problem* (Aufgabe), like proof-event, is not a bearer of any truth-value from the outset. On the other hand, Kolmogorov's logic of problems admits computational accounts of the proving process.

Finally, we exposed the intented interpretations for our logical model from the fields of automated theorem-proving (Kumo system) and Web-based collective proving (Polymath). Moreover, in the formulation of certain aspects of our model, we take into account the conclusions drawn from a mental experiment, described in [Stefaneas et al 2015], in order to explore the specifics of collective problem solving, discovery and creativity, using also ideas from cognitive architectures.

## Acknowledgements

The authors are also grateful to Dr Harry Foundalis and Prof Maricarmen Martinez Baldares (Universidad de los Andes, Colombia) for their constructive readings and valuable comments on certain aspects of this paper.

## References

Aczel, Amir D. 1997. *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem*. Delta (first published 1996).

Bashmakova, Izabella and Smirnova Galina. 2000. *The Beginnings and Evolution of Algebra*. Translated from the Russian by Abe Shenitzer with the editorial assistance of David A. Cox. The Mathematical Association of America.

Bazhanov, Valentin A. 2011. "Mathematical Proof as a Form of Appeal to a Scientific Community," *Russian Studies in Philosophy*, vol. 50, no. 4 (Spring 2012), pp. 52–72.

Davidson, Donald. 1967b, "Causal Relations", *Journal of Philosophy*, **64**, pp. 691–703; reprinted in: Casati, R., and Varzi, A.C. (eds.), *Events*, Dartmouth, Aldershot, 1996, pp. 401–13, and in" Davidson, D., *Essays on Actions and Events*, Oxford: Clarendon Press, 1980, pp. 149–62.

Demidov, Sergei S. (Демидов С. С.). 1966. «К истории проблем Гильберта» [On the history of Hilbert's problems], *Историко-математические исследования*, **17**, pp. 91-122 (in Russian).

—— 2001. ««Математические проблемы» Гильберта и математика XX века» ["Hilbert's mathematical problems" and mathematics of the 20th century], *Историко-математические исследования*, **41** (6), pp. 84-99 (in Russian).

Fauconnier, Gilles and Mark Turner. 2008. *The way we think: Conceptual blending and the mind's hidden complexities*. Basic Books.

Goguen, Joseph A. 1999a. "An introduction to algebraic semiotics, with applications to user interface design". In Nehaniv, C. (ed.), *Computation for Metaphors, Analogy and Agents*. Springer, pp. 242-291.

—— 1999b. "Social and Semiotic Analyses for Theorem Prover User Interface Design", *Formal Aspects of Computing* **11**, pp. 272–301. (Special Issue on User Interfaces for Theorem Provers.)

—— 2001. "What is a proof", http://cseweb.ucsd.edu/~goguen/papers/proof.html

—— 2003. "Semiotic morphisms, representations, and blending for interface design". *Proceedings, AMAST Workshop on Algebraic Methods in Language Processing*. AMAST Press. 1–15. Conference held in Verona, Italy, 25-27 August.

Goguen, Joseph A. and Harell, D. Fox. 2004a. "Style as a choice of blending principles". Shlomo Argamon, Shlomo Dubnov, and Julie Jupp (Eds), *Style and Meaning in Language, Art Music and Design*, AAAI Press, pp. 49-56.

—— 2004b. "Information Visualization and Semiotic Morphisms," in *Multidisciplinary Approaches to Visual Representations and Interpretations*, Grant Malcolm (Ed.) Oxford: Elsevier, pp. 83-98.

—— 2010. "Style: A Computational and Conceptual Blending-Based Approach", Shlomo Argamon, Kevin Burns, Shlomo Dubnov (Eds), *The Structure of Style. Algorithmic Approaches to Understanding Manner and Meaning*. Springer, pp. 291-316.

Hales, Alfred, and Robert Jewett. 1963. "Regularity and Positional Games." *Transactions of the American Mathematical Society* **106**, pp. 222–29.

Henkin, L. Monk, J.D. and Tarski, A. 1971. *Cylindric Algebras*, Part I, North-Holland.

Heyting, A. (1931) "The intuitionist foundations of mathematics," reprinted in: P. Benacerraf and H. Putnam (eds) *Philosophy of Mathematics: Selected Readings,* 2nd ed, Cambridge: Cambridge University Press, 1983, pp. 52–61.

—— 1955. *Les Fondements des Mathématiques. Intuitionnisme. Théorie de la Démonstration.* Paris : Gauthier-Villars. Title of the original: *Mathematische Grundlagenforschung. Intuitionismus. Beweistheorie*. Springer-Verlag, Berlin, 1934.

—— 1956. *Intuitionism: An Introduction*, Amsterdam: North-Holland Publishing, 3rd revised edition, 1971.

—— 1958. "Intuitionism in mathematics", in: R. Klibansky (ed.), *Philosophy in the Mid-Century. A survey* (La Nuova Italia Editrice, Firenze) 101-115.

Huntington, E.V. 1933a. "New sets of independent postulates for the algebra of logic", *Transactions of American Mathematical Society* **35**, pp. 274-304.

—— 1933b. "Boolean algebra: A correction", *Transactions of American Mathematical Society* **35**, pp. 557-558.

Kauffman, Louis H. 1990. "Robbins Algebra". *Proceedings of the Twentieth International Symposium on Multiple Valued Logic*. IEE Computer Society Press, pp. 54-60.

—— 2001. "The Robbins Problem: computer proofs and human proofs" *Kybernetes - The International Journal of Systems and Cybernetics, Gordon Pask Remembered and Celebrated: Part I*, Bernard Scott and Ranulph Glanville (eds), **30** (5/6), pp.726-752.

Kleene, Stephen Cole. 1945. "On the interpretation of intuitionistic number theory", *Journal of Symbolic Logic*, 10, 109-124.

Klein, Jacob. 1968. *Greek Mathematical Thought and the Origin of Algebra*. Translated by Eva Brann from the German original *Griechische Logistik und die Entstehung der Algebra*. Reprinted by Dover, 1992.

Kleiner Israel. 2000. "From Fermat to Wiles: Fermat's Last Theorem Becomes a Theorem". *Elemente der Mathematik* **55**, pp. 19-37.

Kolmogorov, Andrei N. 1932. „Zur Deutung der intuitionistischen Logik", *Mathematische Zeitschrift* **35**, pp. 58–65. English translation in V.M. Tikhomirov (ed.) *Selected Works of A.N. Kolmogorov*. Vol. I: *Mathematics and Mechanics*, 151-158. Kluwer, Dordrecht, 1991.

—— 1988. "Letters of A. N. Kolmogorov to A. Heyting", *Успехи математических наук* (*Uspekhi Matematicheskikh Nauk*)*,* **43** (6), pp. 75-77; English translation, *Russian Mathematical Surveys*, **43** (6), pp. 89-93.

Kowalski, Robert. 1992. "Database updates in the event calculus", *Journal of Logic Programming*, **12**, 121-146.

Kowalski, Robert and Sergot Marek. 1986 “A Logic-Based Calculus of Events”, *New Generation Computing* **4**, pp. 67–95.
McCune, William. 1997. “Solution of the Robbins Problem”, *Journal of Automated Reasoning* **19**(3), pp. 263-76.
Mac Lane, Saunders. 1997. “Despite Physicists, Proof is Essential in Mathematics”, *Synthese* **111**, pp. 147–154.
Martin-Löf, Per. 1984. *Intuitionistic type theory*. (Notes by Giovanni Sambin of a series of lectures given in Padua, June 1980). Napoli, Bibliopolis.
Medvedev, Yu. 1962. “Finite problems”, *Soviet Mathematics Doklady*, **3**, 227-230.
Polymath. 2009. *A New Proof of the Density Hales-Jewett Theorem*. At http://arxiv.org/abs/0910.3926, arXiv:0910.3926v2 [math.CO], accessed April 2, 2012.
—— 2010a. *Deterministic Methods to Find Primes*. At http://arxiv.org/abs/1009.3956, arXiv:1009.3956v3 [math.NT], accessed April 2, 2012.
—— 2010b. *Density Hales-Jewett and Moser Numbers*. At http://arxiv.org/abs/1002.0374, arXiv:1002.0374v2 [math.CO], accessed April 2, 2012.
Rudin, Walter. 1953. *Principles of Mathematical Analysis,* New York: McGraw-Hill.
Miller, Rob and Shanahan Murray. 1999. “The event-calculus in classical logic — alternative axiomatizations”, *Electronic Transactions on Artificial Intelligence* **3**(1), pp. 77-105.
Singh, Simon. 1998. *Fermat’s Enigma*. New York: Anchor Books.
Stefaneas, Petros and Vandoulakis, Ioannis. 2012. “The Web as a Tool for Proving” *Metaphilosophy*. Special Issue: Philoweb: Toward a Philosophy of the Web: Guest Editors: Harry Halpin and Alexandre Monnin. Volume 43, Issue 4, pp. 480–498. Reprinted in: Harry Halpin and Alexandre Monnin (Eds) *Philosophical Engineering: Toward a Philosophy of the Web*. Wiley-Blackwell, 2014, pp. 149-167.
—— 2014. Proofs as spatio-temporal processes”, Pierre Edouard Bour, Gerhard Heinzmann, Wilfrid Hodges and Peter Schroeder-Heister (Eds) “Selected Contributed Papers from the 14th International Congress of Logic, Methodology and Philosophy of Science”, *Philosophia Scientiæ*, **18**(3), pp. 111-125.
Stefaneas Petros, Vandoulakis Ioannis, Martínez Maricarmen and Foundalis Harry. 2012. “Web-Based Mathematical Problem-Solving with Codelets”, *Computational Creativity, Concept Invention, and General Intelligence* Tarek R. Besold, Kai-Uwe Kuehnberger, Marco Schorlemmer, Alan Smaill (Eds.), pp. 38–41.
—— 2015. “Collective Discovery Events: Web-based Mathematical Problem-solving with Codelets”. In: Tarek R. Besold, Marco Schorlemmer, Alan Smaill (Eds) *Computational Creativity Research: Towards Creative Machines*. Atlantis Thinking Machines (Book 7) Atlantis/Springer, pp. 371-392.
Tieszen, R. L. 1989. *Mathematical Intuition: Phenomenology and Mathematical Knowledge*, Dordrecht: Kluwer.
—— 1992. “What is a Proof?” In: Detlefsen, M. (ed.) *Proof, Logic and Formalization*, London: Routledge. pp. 57–76.
—— 2000. “Intuitionism, Meaning Theory and Cognition”, *History and Philosophy of Logic* **21**, pp. 179–194.
—— 2005. *Phenomenology, Logic, and the Philosophy of Mathematics*. Cambridge: Cambridge University Press.
Vandoulakis, Ioannis. 1998. “Was Euclid’s Approach to Arithmetic Axiomatic?” *Oriens–Occidens* Cahiers du Centre d’histoire des Sciences et des philosophies arabes et Médiévales*,* **2** (1998), pp. 141-181.

—— 2009. “Styles of Greek arithmetic reasoning,” 数学史の研究 Study of the History of Mathematics RIMS 研究集会報告集 *Kôkyûroku* No 1625, pp. 12-22.
—— 2010. “A Genetic Interpretation of Neo-Pythagorean Arithmetic,” *Oriens–Occidens* Cahiers du Centre d’histoire des Sciences et des philosophies arabes et Médiévales*,* **7** (2010), pp. 113-154.
—— 2015. “On A.A. Markov’s attitude towards Brouwer’s intuitionism”, Pierre Edouard Bour, Gerhard Heinzmann, Wilfrid Hodges and Peter Schroeder-Heister (Eds) “Proceedings of the 14th Congress of Logic, Methodology and Philosophy of Science”, *Philosophia Scientiæ*, **19**(1), pp. 143-158.
Vandoulakis, Ioannis & Stefaneas, Petros. 2013a. “Conceptions of proof in mathematics”, B.A. Бажанов А.Н. Кричевец, В.А. Шапошников (ред.) *Доказательство. Очевидность, достоверность и убедительность в математике. [Proof. Evidence, reliability and convincingness].* Труды Московского семинара по философии математики, pp. 256-281.
—— 2013b. “Proof-events in History of Mathematics”, *Gaṇita Bhāratī*, **35** (1-4), 2013, 257-295.
—— 2014. “On the semantics of proof-events”, *Труды XII Международных Колмогоровских Чтений* (*Proceedings of the 12th International Kolmogorov Conference*), 20-23 May 2014, Yaroslavl’, Russia, pp. 137-144.
Winker, Steven K. 1990. “Robbins Algebra: Conditions That Make a Near-Boolean Algebra Boolean”, *Journal of Automated Reasoning* **6**(4), pp. 465-489.
—— 1992. “Absorption and idempotency criteria for a problem in near-Boolean algebras”, *Journal of Algebra* **153** (2), pp. 414-423.