Mathematical Proof and Many-Valued Logic

Dexue Zhang (张德学)

School of Mathematics, Sichuan University

2020年全国数理逻辑年会, 南开大学

Outline

Mathematical proof

The aim of a proof is to convince other people that something is true. So, a proof follows some “styles”.

A mathematical proof is a finite sequence of assertions of which each term is either an axiom or is **deducted** from the preceding ones.

A syllogism (a deduction) is discourse in which, certain things being stated, something other than what is stated follows of necessity from their being so.

— Aristotle, Prior Analytics

Examples of syllogism (inference rule)

Modus ponens

$$\frac{\begin{array}{l} p \to q \\ p \end{array}}{q}$$

The law of double negation (proof by contradiction)

$$\frac{\neg\neg p}{p}$$

The law of excluded middle

$$\frac{}{p \vee \neg p}$$

Proof by contradiction is “one of a mathematician’s finest weapons”. (G. H. Hardy)

But, not everyone is happy with this weapon.

Intuitionism

Intuitionism, introduced by Brouwer, is sometimes and rather simplistically characterized by saying that its adherents refuse to use the law of excluded middle in mathematical reasoning.

The law of excluded middle is related to the *a priori* assumption that every mathematical problem has a solution.

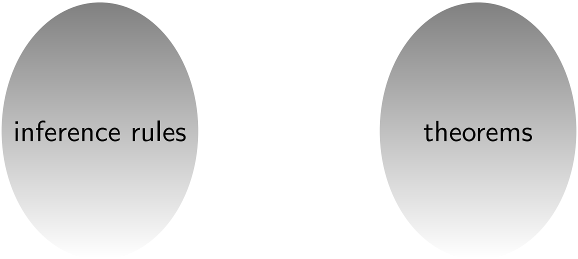
In intuitionistic logic, which codifies Brouwer's way of doing mathematics, the law of excluded middle is equivalent to the law of double negation. Thus, proof by contradiction is not allowed in intuitionism either.

While intuitionism focuses on what can be proved without resort to the law of excluded middle, this talk is concerned with:

What cannot be proved if proof by contradiction is not allowed?

In other words, are there "theorems" that can be proved only when proof by contradiction is allowed?

A general problem is to investigate the dependence of a “theorem” on a specific inference rule.



We'll present two examples in order theory.

The idea is as follows: to see whether or not a "theorem" depends on a specific inference rule, we construct a portion of the mathematical world so that

- the "internal logic" satisfies (or dissatisfies) that specified inference rule;
- the "theorem" can be formulated therein.

We'll present two examples in order theory.

The idea is as follows: to see whether or not a "theorem" depends on a specific inference rule, we construct a portion of the mathematical world so that

- the "internal logic" satisfies (or dissatisfies) that specified inference rule;
- the "theorem" can be formulated therein.

Algebraization of logic, initiated by George Boole, makes this possible.

Outline

Lattice

Let X be a set. A partial order on X is a binary relation $\leq$ on X that is

- reflexive,
- transitive, and
- antisymmetric.

A partially ordered set $(X, \leq)$ is a lattice if

- it has a least and a greatest element, denoted by 0 and 1, respectively;
- every pair of elements x, y in X has a join and a meet, denoted by $x \vee y$ and $x \wedge y$, respectively.

Galois connection

Let X, Y be partially ordered sets; let $f : X \longrightarrow Y$ and $g : Y \longrightarrow X$ be maps. We say that f is a left adjoint of g, or g is a right adjoint of f, if

$$f(x) \leq y \iff x \leq g(y)$$

for all $x \in X$ and $y \in Y$.

In this case we say the pair (f, g) is a Galois connection (or, an adjunction) and write

$$f \dashv g.$$

Heyting algebra

Definition 1

A Heyting algebra is a lattice L such that for each $x \in L$, the map

$$x \wedge - : L \longrightarrow L, \quad z \mapsto x \wedge z$$

has a right adjoint

$$x \rightarrow - : L \longrightarrow L, \quad y \mapsto x \rightarrow y.$$

For all x, y, z in a Heyting algebra,

$$x \wedge z \leq y \iff z \leq x \to y.$$

So a Heyting algebra can be treated as a table of truth values, with $\wedge$ and $\to$ modelling the connectives conjunction and implication, respectively.

In particular, the inequality

$$x \wedge (x \to y) \leq y$$

is an algebraization of Modus Ponens.

The element $x \to 0$ is called the negation of x and is denoted by

$$\neg x.$$

Boolean algebra

A lattice L is distributive if it satisfies the distributive law:

$$\forall x, y, z \in L, \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

Let x, y be elements of a lattice L. We say that y is a *complement* of x if

$$x \wedge y = 0 \quad \text{and} \quad x \vee y = 1.$$

Boolean algebra

A lattice L is distributive if it satisfies the distributive law:

$$\forall x, y, z \in L, \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

Let x, y be elements of a lattice L. We say that y is a *complement* of x if

$$x \wedge y = 0 \quad \text{and} \quad x \vee y = 1.$$

Definition 2

A Boolean algebra is a distributive lattice of which every element has a complement.

Proposition 3

For a lattice L, the following conditions are equivalent:

(1) *L is a Boolean algebra.*

(2) *L is a Heyting algebra that satisfies the law of excluded middle in the sense that $x \vee \neg x = 1$ for all $x \in L$.*

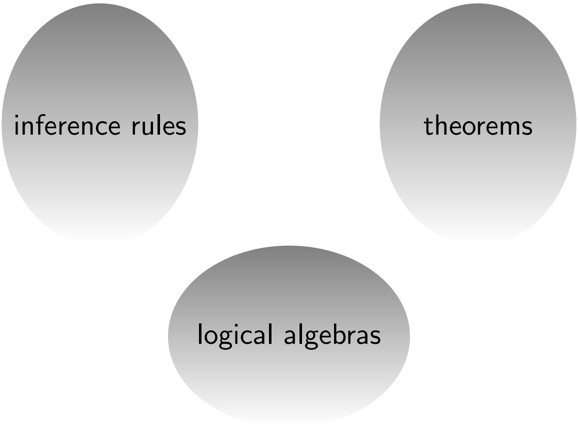
(3) *L is a Heyting algebra that satisfies the law of double negation in the sense that $x = \neg\neg x$ for all $x \in L$.*

Logical algebras, many-valued logics

Classic logic	Boolean algebra (G. Boole)
Intuitionistic logic	Heyting algebra (A. Heyting)
Łukasiewicz logic	MV-algebra (C.C. Chang)
BL-logic	BL-algebra (P. Hájek)
......	......

It can be said, to some extent, that a many-valued logic is a logic that is weaker than the classical one but applicable to a wider context.

What can be and what cannot be proved in mathematics based on a "many-valued logic"?



Logical algebras are "carriers of inference rules".

Quantale: a general form of logical algebra

A quantale (a commutative quantale, to be precise)

$$\mathsf{Q} = (\mathsf{Q}, \&, k)$$

is a commutative monoid with k being the unit, such that the underlying set Q is a complete lattice and the multiplication & distributes over arbitrary joins.

The unit k need not be the top element in Q. When k happens to be the top element, Q is called *integral*.

Since & distributes over arbitrary joins, it determines a binary operation $\to$ via the adjoint property:

$$p \,\&\, q \leq r \iff q \leq p \to r.$$

Because of this adjunction, every quantale can be thought of as a "logical algebra":

- k, true;
- $\&$, conjunction;
- $\to$, implication;
- $\bigvee_{x \in X} P(x)$, (the degree that) P holds for some $x \in X$;
- $\bigwedge_{x \in X} P(x)$, (the degree that) P holds for all $x \in X$.

F.W. Lawevere, Metric spaces, genetalized logic, and closed categories, Rendiconti del Seminario Matématico e Fisico di Milano 43 (1973) 135-166.

Let Q be an *integral* quantale. We say that Q satisfies the law of double negation if

$$(p \to 0) \to 0 = p$$

for all $p \in Q$.

Example of quantales

1. Complete Boolean algebras.
2. Complete Heyting algebras.
3. Complete MV-algebras in the sense of C.C. Chang.
   Actually, a complete MV-algebra is a quantale such that for all x, y,
   $$x \& (x \to y) = x \wedge y \quad \text{and} \quad (x \to 0) \to 0 = x.$$
4. Lawvere's quantale: $([0, \infty]^{\mathrm{op}}, +, 0)$.

Example of quantales: continuous t-norm

A continuous t-norm on $[0,1]$ is a continuous function

$$\& : [0,1] \times [0,1] \longrightarrow [0,1]$$

such that

$$([0,1], \&, 1)$$

is a quantale.

- Gödel t-norm:

$$x \,\&\, y = \min\{x, y\}, \quad x \to y = \begin{cases} 1, & x \le y, \\ y, & x > y. \end{cases}$$

  The implication $\to$ is continuous except at (x, x), $x < 1$.

- Product t-norm:

$$x \,\&\, y = x \cdot y, \quad x \to y = \begin{cases} 1, & x \le y, \\ y/x, & x > y. \end{cases}$$

  The implication $\to$ is continuous except at $(0, 0)$.

- Łukasiewicz t-norm:

$$x \,\&\, y = \max\{x + y - 1, 0\}, \quad x \to y = \min\{1 - x + y, 1\}.$$

  The implication $\to$ is continuous on $[0, 1]^2$.

Our task

In order theory, it is well-known that

- the complete distributivity law is self-dual in the sense that the opposite of a completely distributive lattice is completely distributive;
- every completely distributive lattice is a domain (i.e., a continuous directed complete partially ordered set).

We are to demonstrate that these conclusions depend on certain inference rules.

Specifically, let $\mathsf{Q} = (\mathsf{Q}, \&, k)$ be a quantale. We'll

- formulate the notions of complete distributive lattices and domains in the Q-valued context;
- investigate the dependence of the self-duality of complete distributivity law on the logic features of Q;
- investigate whether every completely distributive lattice is a domain in the Q-valued context.

Theorem 4

Let $\mathsf{Q} = (\mathsf{Q}, \&, k)$ *be an integral quantale. Then the following statements are equivalent:*

(1) *If* A *is a completely distributive* Q*-lattice, then so is its opposite* A^{op}*.*

(2) Q *satisfies the law of double negation.*

Theorem 5

Let $\&$ *be a continuous t-norm and* $\mathsf{Q} = ([0,1], \&, 1)$*. Then the following statements are equivalent:*

(1) *Every completely distributive* Q*-lattice is a* Q*-domain.*

(2) *The implication* $\rightarrow : [0,1]^2 \longrightarrow [0,1]$ *is continuous at every point off the diagonal.*

Outline

Completely distributive lattice

A partially ordered set X is a complete lattice if every subset of X, including the empty one, has a join. This is equivalent to that every subset of X, including the empty one, has a meet.

A complete lattice X is completely distributive if it satisfies the complete distributivity law in the sense that for any family $\{x_{i,j} \mid i \in I, j \in J_i\}$ of elements of X,

$$\bigwedge_{i \in I} \bigvee_{j \in J_i} x_{i,j} = \bigvee_{f \in \prod_{i \in I} J_i} \bigwedge_{i \in I} x_{i,f(i)}.$$

Let X be a partially ordered set; let $\mathcal{P}X$ be the set of all lower sets of X endowed with the inclusion order. Then X is a complete lattice if and only if the map

$$\mathrm{y} : X \longrightarrow \mathcal{P}X, \quad x \mapsto {\downarrow} x$$

has a left adjoint

$$\sup : \mathcal{P}X \longrightarrow X, \quad A \mapsto \bigvee A,$$

which sends a subset to its join.

Lemma 6 (Characterizing the CD law by Galois connection)

For a partially ordered set X, the following conditions are equivalent:

(1) *X is a completely distributive lattice;*

(2) *X is a complete lattice and*

$$\bigwedge_{i \in I} \sup A_i = \sup \bigcap_{i \in I} A_i$$

for each family $\{A_i\}_{i \in I}$ of lower sets of X;

(3) *There is a string of adjunctions*

$$\Downarrow \dashv \sup \dashv \mathsf{y} : X \longrightarrow \mathcal{P}X.$$

Theorem 7

If a complete lattice X is completely distributive, then so is the opposite of X.

Theorem 7

If a complete lattice X is completely distributive, then so is the opposite of X.

The following facts are needed in the proof of this theorem.

Given elements x, y in a complete lattice L, we say that x is totally below y and write $x \lhd y$ if, for any subset A of L, $y \leq \bigvee A$ implies that $x \leq a$ for some $a \in A$.

If A is a completely distributive lattice, then for each $x \in A$, $\Downarrow x$ is the set of elements that are totally below x and $x = \sup \Downarrow x$.

The totally below relation in a completely distributive lattice is interpolative in the sense that

$$x \lhd y \;\Rightarrow\; \exists z, x \lhd z \lhd y.$$

Proof of the self-duality of the CD law

It suffices to check that for each family $\{A_i\}_{i\in I}$ of upper sets in X,

$$\inf \bigcap_{i\in I} A_i = \bigvee_{i\in I} \inf A_i.$$

We only need to check that the left side $\leq$ the right side. To this end, we check that if x is totally below $\inf \bigcap_{i\in I} A_i$, then $x \leq \inf A_i$ for some $i \in I$. Suppose on the contrary that $x \not\leq \inf A_i$ for any $i \in I$. Pick z such that $x \lhd z \lhd \inf \bigcap_{i\in I} A_i$; for each i pick some $a_i \in A_i$ with $x \not\leq a_i$. Since each A_i is an upper set, it follows that

$$\bigvee_{i\in I} a_i \in \bigcap_{i\in I} A_i.$$

Thus, $z \not\leq \bigvee_{i\in I} a_i$, contradicting that $z \leq \inf \bigcap_{i\in I} A_i$.

Outline

Q-ordered sets

Let $\mathsf{Q} = (\mathsf{Q}, \&, k)$ be quantale. A Q-*ordered set* consists of a set A and a map $\alpha : A \times A \longrightarrow \mathsf{Q}$ such that

$$k \leq \alpha(x, x) \quad \text{and} \quad \alpha(y, z) \,\&\, \alpha(x, y) \leq \alpha(x, z)$$

for all $x, y, z \in A$.

We often write A for the pair (A, α) and write $A(x, y)$ for $\alpha(x, y)$.

A map $f : A \longrightarrow B$ between Q-ordered sets preserves Q-order if

$$A(x_1, x_2) \leq B(f(x_1), f(x_2))$$

for all $x_1, x_2 \in A$.

In the terminology of category theory,

- a quantale Q is a symmetric, monoidal closed and complete small category;
- the category of Q-ordered sets and Q-order-preserving maps is the category of categories and functors enriched over Q.

A Q-ordered set A is called separated, or antisymmetric, if

$$A(x, y) \geq k, A(y, x) \geq k \quad \Rightarrow \quad x = y.$$

All Q-ordered sets are assumed to be separated in the sequel.

Example 8

- For Lawvere's quantale $\mathsf{Q} = ([0, \infty]^{\mathrm{op}}, +, 0)$, Q-ordered sets and Q-order-preserving maps are precisely quasi-metric spaces (with distance allowed to be infinity) and Lipschitz maps with Lipschitz constant 1.
- For the quantale $\mathsf{Q} = ([0, 1], \min, 1)$, a Q-ordered set is essentially a quasi-ultrametric space.

Adjunction (enriched Galois connection)

Let $f : A \longrightarrow B$ and $g : B \longrightarrow A$ be maps between Q-ordered sets. We say that f is left adjoint to g, or g is right adjoint to f, if

$$B(f(x), y) = A(x, g(y))$$

for all $x \in A$ and $y \in B$. In this case we say that the pair (f, g) is an adjunction and write

$$f \dashv g.$$

The Q-ordered set of lower Q-sets

Let A be a Q-ordered set. A lower Q-set of A is a map

$$\phi : A \longrightarrow \mathsf{Q}$$

such that

$$\phi(y) \,\&\, A(x,y) \leq \phi(x).$$

Let

$$\mathcal{P}A$$

be the set of lower Q-sets of A. There is a natural Q-order on $\mathcal{P}A$ — the inclusion Q-order, given by

$$\mathcal{P}A(\phi_1, \phi_2) = \bigwedge_{x \in A} \phi_1(x) \to \phi_2(x).$$

Let $f : A \longrightarrow B$ be a map that preserves Q-order. Define

$$f^{\rightarrow} : \mathcal{P}A \longrightarrow \mathcal{P}B \quad \text{and} \quad f^{\leftarrow} : \mathcal{P}B \longrightarrow \mathcal{P}A$$

by

$$f^{\rightarrow}(\phi)(y) = \bigvee_{x \in A} \phi(x) \,\&\, B(y, f(x))$$

and

$$f^{\leftarrow}(\psi)(x) = \psi(f(x)).$$

Then

$$f^{\rightarrow} \dashv f^{\leftarrow}.$$

This adjunction is a special case of (enriched) Kan extension in category theory.

Yoneda embedding

For each $a \in A$, $\mathrm{y}(a) := A(-, a)$ is a lower Q-set of A.

Lemma 9 (Yoneda lemma)

For all $a \in A$ and $\phi \in \mathcal{P}A$, $\mathcal{P}A(\mathrm{y}(a), \phi) = \phi(a)$.

Thus, $a \mapsto \mathrm{y}(a)$ defines an embedding

$$\mathrm{y} : A \longrightarrow \mathcal{P}A,$$

which is known as the Yoneda embedding.

Definition 10

Let A be a Q-ordered set. We say that A is a complete Q-lattice if the Yoneda embedding

$$\mathrm{y} : A \longrightarrow \mathcal{P}A$$

has a left adjoint

$$\sup : \mathcal{P}A \longrightarrow A.$$

That is to say, for each $\phi \in \mathcal{P}A$, there is an element $\sup \phi$ of A such that

$$A(\sup \phi, x) = \mathcal{P}A(\phi, \mathrm{y}(x))$$

for all $x \in A$.

Intuitively, $\sup \phi$ is the least upper bound of the lower Q-set ϕ.

Outline

Definition 11

A Q-ordered set A is a completely distributive Q-lattice if there is a string of adjunctions

$$\mathsf{t} \dashv \sup \dashv \mathsf{y} : A \longrightarrow \mathcal{P}A.$$

Definition 11

A Q-ordered set A is a completely distributive Q-lattice if there is a string of adjunctions

$$\mathsf{t} \dashv \sup \dashv \mathsf{y} : A \longrightarrow \mathcal{P}A.$$

Example 12

For each Q-ordered set A, $\mathcal{P}A$ is completely distributive, because

$$\mathsf{y}_A^{\rightarrow} \dashv \mathsf{y}_A^{\leftarrow} \dashv \mathsf{y}_{\mathcal{P}A} : \mathcal{P}A \longrightarrow \mathcal{P}\mathcal{P}A.$$

I. Stubbe, Towards "dynamic domains": Totally continuous cocomplete $\mathcal{Q}$-categories, Theoretical Computer Science 373 (2007) 142-160.

Theorem 13

For each integral quantale Q*, the following statements are equivalent:*

(1) *If* A *is a completely distributive* Q*-lattice, then so is its opposite* A^{op}*.*

(2) Q *satisfies the law of double negation.*

- H. Lai, On the Order Structure Properties of Ω-categories, Thesis, Sichuan University, 2007.
- H. Lai, L. Shen, Regularity vs. constructive complete (co)distributivity, Theory and Applications of Categories 33 (2018) 492–522.

Outline

Consider the formulas:

$$\exists x(p \to q(x))$$

and

$$p \to \exists x q(x).$$

Are they "logically equivalent"?

Domains

Let X be a partially ordered set; and let $\mathsf{Idl}(X)$ be the set of all ideals (= directed lower sets) of X. We say that

- X is a **d**irected **c**omplete **p**artially **o**rdered set if the map

  $$\mathsf{y} : X \longrightarrow \mathsf{Idl}(X), \quad x \mapsto \downarrow x$$

  has a left adjoint

  $$\sup : \mathsf{Idl}(X) \longrightarrow X, \quad I \mapsto \bigvee I;$$

- X is a domain if there is a string of adjunctions

  $$\Downarrow \dashv \sup \dashv \mathsf{y} : X \longrightarrow \mathsf{Idl}(X).$$

Theorem 14

Every completely distributive lattice is a domain.

G. Gierz, K.H. Hofmann, K. Keimel, J.D. Lawson, M. Mislove, D.S. Scott, Continuous Lattices and Domains, Encyclopedia of Mathematics and its Applications, Vol. 93, Cambridge University Press, Cambridge, 2003.

A fact:

Let X be a partially ordered set. Then a lower set I of X is an ideal if and only if it is nonempty and is irreducible in the sense that for any lower sets A and B,

$$I \subseteq A \cup B \;\Rightarrow\; \text{either } I \subseteq A \text{ or } I \subseteq B.$$

Q-domain

Let A be a Q-ordered set. An irreducible ideal of A is a lower Q-set ϕ of A such that

- $\bigvee_{x \in A} \phi(x) \geq k$;
- for any lower Q-sets ψ_1 and ψ_2 of A,

$$\mathcal{P}A(\phi, \psi_1 \vee \psi_2) = \mathcal{P}A(\phi, \psi_1) \vee \mathcal{P}A(\phi, \psi_2).$$

Q-domain

Let A be a Q-ordered set. An irreducible ideal of A is a lower Q-set ϕ of A such that

- $\bigvee_{x \in A} \phi(x) \geq k$;
- for any lower Q-sets ψ_1 and ψ_2 of A,

$$\mathcal{P}A(\phi, \psi_1 \vee \psi_2) = \mathcal{P}A(\phi, \psi_1) \vee \mathcal{P}A(\phi, \psi_2).$$

Example 15

For each $a \in A$, $\mathrm{y}(a) = A(-, a)$ is an irreducible ideal of A.

For each Q-ordered set A, let $\mathcal{I}A$ be the subset of $\mathcal{P}A$ consisting of irreducible ideals of A. Since the Yoneda embedding $\mathrm{y} : A \longrightarrow \mathcal{P}A$ factors through $\mathcal{I}A$, we have a map

$$\mathrm{y} : A \longrightarrow \mathcal{I}A, \quad a \mapsto A(-, a).$$

For each Q-ordered set A, let $\mathcal{I}A$ be the subset of $\mathcal{P}A$ consisting of irreducible ideals of A. Since the Yoneda embedding $\mathrm{y} : A \longrightarrow \mathcal{P}A$ factors through $\mathcal{I}A$, we have a map

$$\mathrm{y} : A \longrightarrow \mathcal{I}A, \quad a \mapsto A(-, a).$$

Definition 16

A Q-ordered set A is a Q-domain if there is a string of adjunctions:

$$\mathrm{d} \dashv \sup \dashv \mathrm{y} : A \longrightarrow \mathcal{I}A.$$

Example 17

1. For each Q-ordered set A, $\mathcal{I}A$ is a Q-domain.
2. Let $\mathsf{Q} = ([0, \infty]^{\mathrm{op}}, +, 0)$. Then a metric space (X, d) (in the usual sense) is a Q-domain if and only if every Cauchy sequence in (X, d) converges.

Is every completely distributive Q-lattice a Q-domain?

Theorem 18

Let & be a continuous t-norm and $\mathsf{Q} = ([0,1], \&, 1)$*. Then the following statements are equivalent:*

(1) *Every completely distributive* Q*-lattice is a* Q*-domain.*

(2) *The implication*

$$\rightarrow : [0,1]^2 \longrightarrow [0,1]$$

is continuous at every point off the diagonal.

H. Lai, D. Zhang, Completely distributive enriched categories are not always continuous, Theory and Application of Categories 35 (2020) 64-88.

H. Lai, D. Zhang, G. Zhang, A comparative study of ideals in fuzzy orders, Fuzzy Sets and Systems 382 (2020) 1-28.

The requirement that

$$\rightarrow : [0,1]^2 \longrightarrow [0,1]$$

is continuous at every point off the diagonal can be rephrased as:

If p is not equivalent to $\exists x q(x)$, then

$$p \rightarrow \exists x q(x)$$

is equivalent to

$$\exists x (p \rightarrow q(x)).$$

Concluding remark

J.B. Rosser and A.R. Turquette raised five questions in:

Many-Valued Logics, North-Holland Publishing Company, Amsterdam, 1952.

The fourth and the fifth are:

- Are there useful applications of many-valued logics?
- Precisely what problems (if any) can be solved by means of many-valued logics which can not be solved by the ordinary two-valued logic?

Concluding remark

J.B. Rosser and A.R. Turquette raised five questions in:

Many-Valued Logics, North-Holland Publishing Company, Amsterdam, 1952.

The fourth and the fifth are:

- Are there useful applications of many-valued logics?
- Precisely what problems (if any) can be solved by means of many-valued logics which can not be solved by the ordinary two-valued logic?

Mathematics based on many-valued logics are useful in the investigation of dependence of a “theorem” on an inference rule.