dialogues,
proofs,
and programs

modified ToLo V tutorial for students of the Savle Tsereteli
Institute of Philosophy, Ilia State University

tadeusz litak
informatik 8, fau erlangen-nürnberg

this tutorial: propositional logic

- we build sentences from atomic pieces of information, i.e., atoms p, q, r …
- example: *p* can be “Snow is falling in Tbilisi on June 13, 2016”. Or perhaps “Tamar Bagrationi was born as the daughter of King George III by his consort Burdukhan”

- complex sentences are obtained using propositional connectives /\, \/ ->, ¬ and perhaps truth constants (**T, F**). I’ll use A, B, C … to range over them

- of course, the scope of logic is broader than that
- many of you have seen quantifiers, at the very least
- in fact, many differences between classical and constructive approaches visible fully only when considering first-order logics, higher-order logics or full-blown type theories
- however, for today just the propositional setting would do: enough differences visible even on this level

our questions

- how to understand logical connectives?
- which sentences are tautologies?
- what do we care about when setting up logical system?

classical answer

- truth value is the only relevant information about atoms (an assignment of truth values often called a valuation)

- there are only two truth values: 0 and 1 (many-valued/fuzzy logics go for [0,1] interval)

- **T** and **F** constantly mapped to 1 and 0, respectively

- logical system is set up so that we never infer 0 from 1

truth tables

->	0	1
0	1	1
1	0	1

∧	0	1
0	0	0
1	0	1

->	0	1
0	0	1
1	1	1

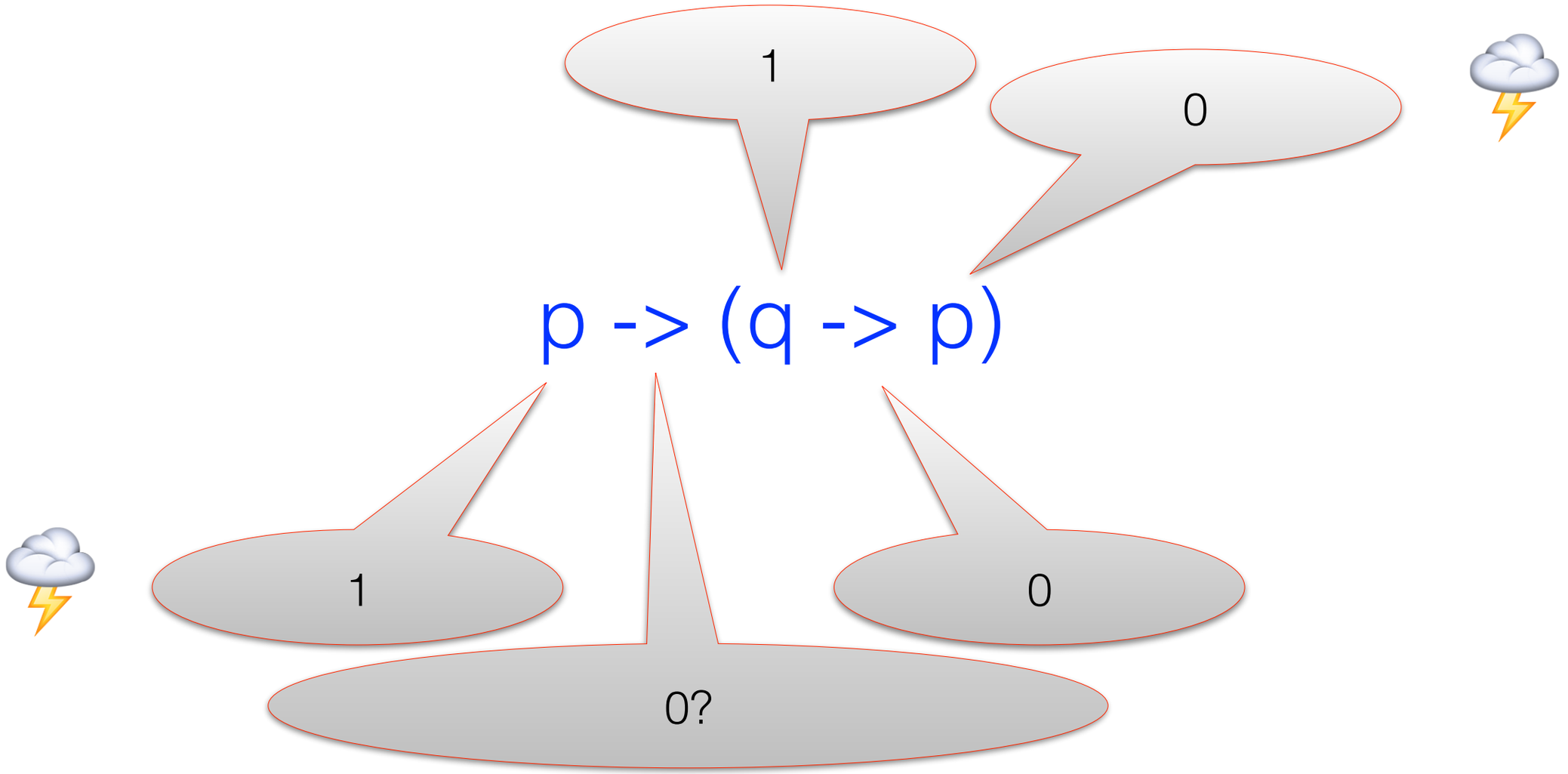
¬	
0	1
1	0

Note: ¬A = A -> **F**.
We can keep this as definition of ¬

how to check for tautologies?

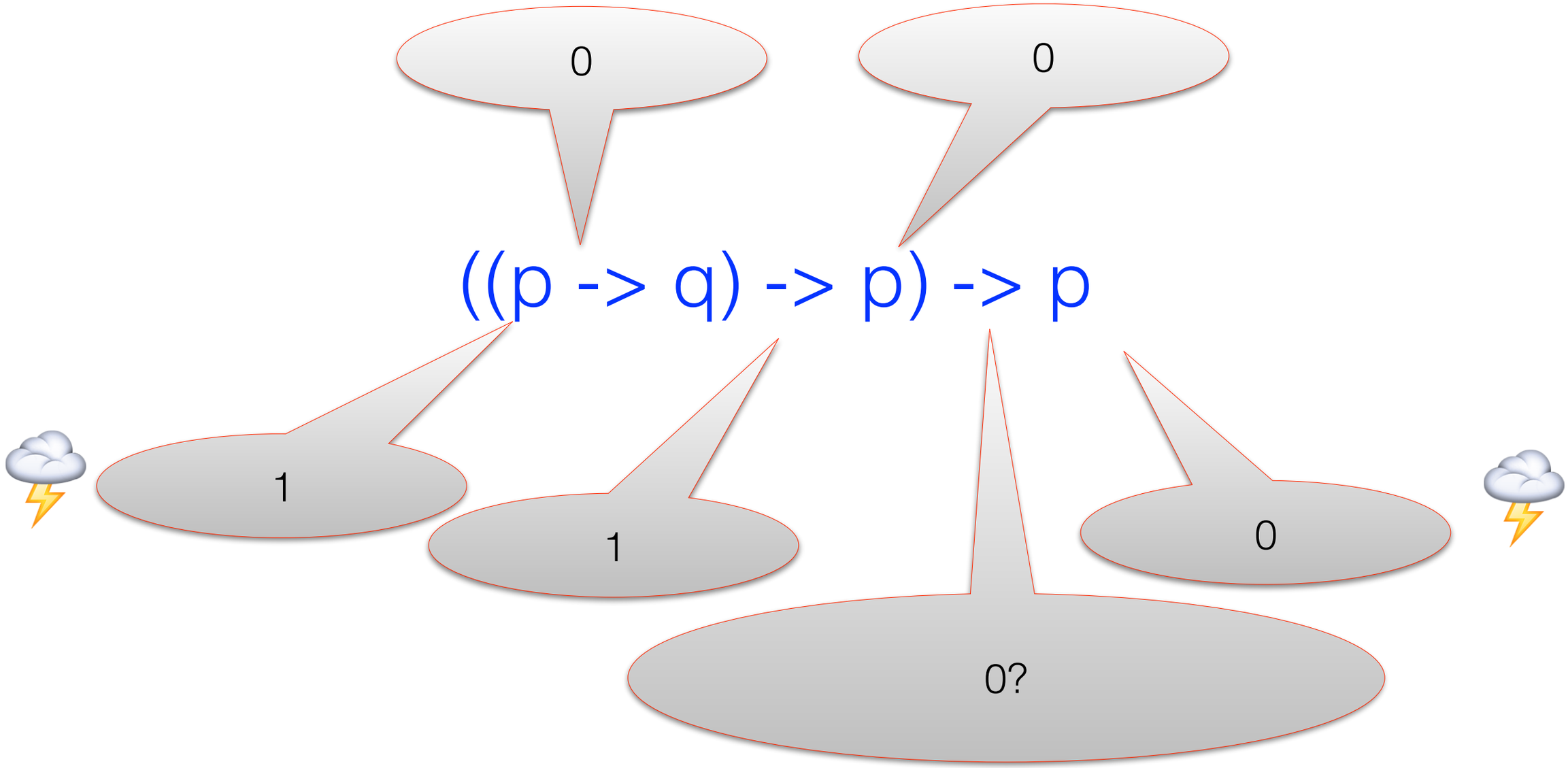
- just one of many possible approaches:
- try to assign 0 to the whole formula and propagate
- mostly deterministic: only one way to make implication, disjunction or negation false, only one way to make conjunction or negation true
- if under all possible valuations, some atom ends with 1 in one occurrence and 0 in another, we got a tautology, otherwise a satisfying valuation

what sentences are tautologies?



Peirce’s law

((p -> q) -> p) -> p



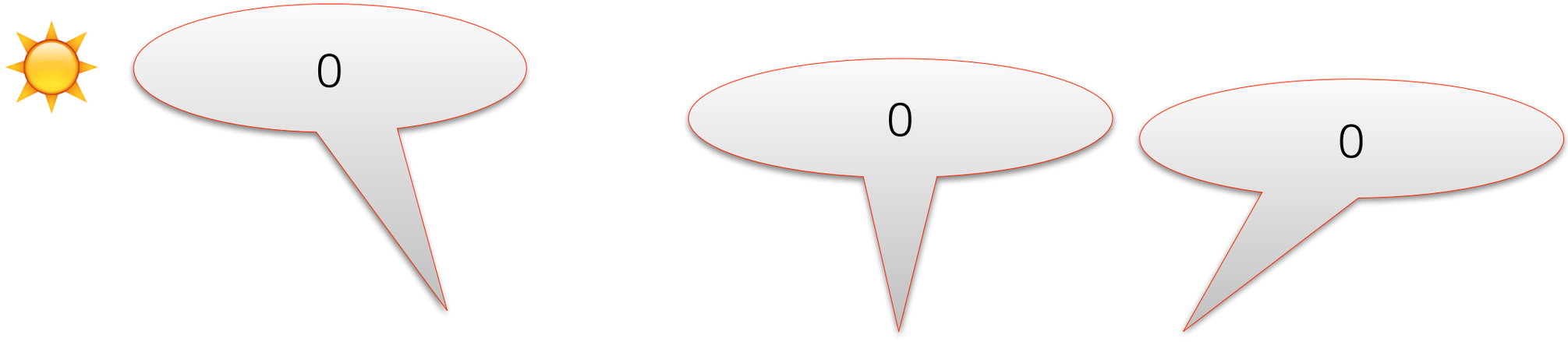
what sentences are tautologies?

(p -> (q -> r)) -> ((p -> q) -> (p -> r)

0 1 0 1 1 1 0

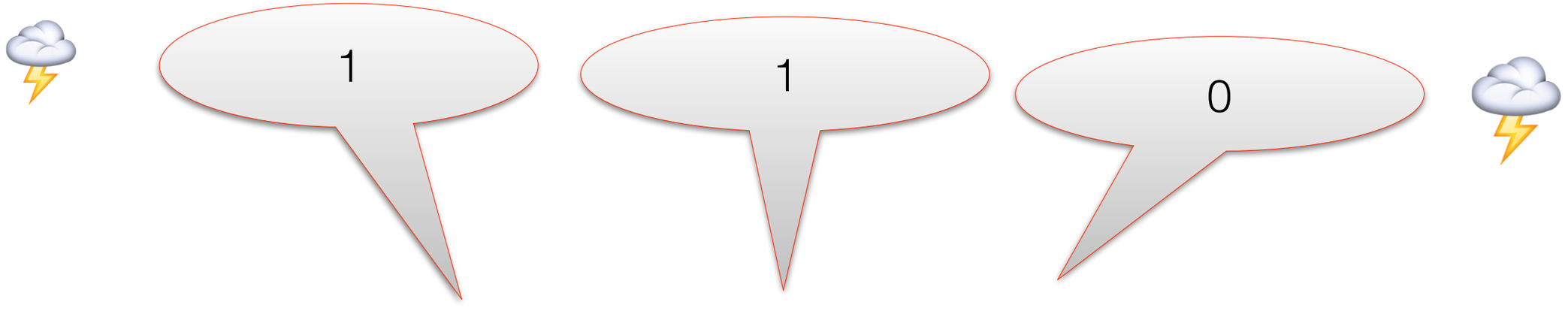
1 0 0 1 0 0 0?

not a tautology

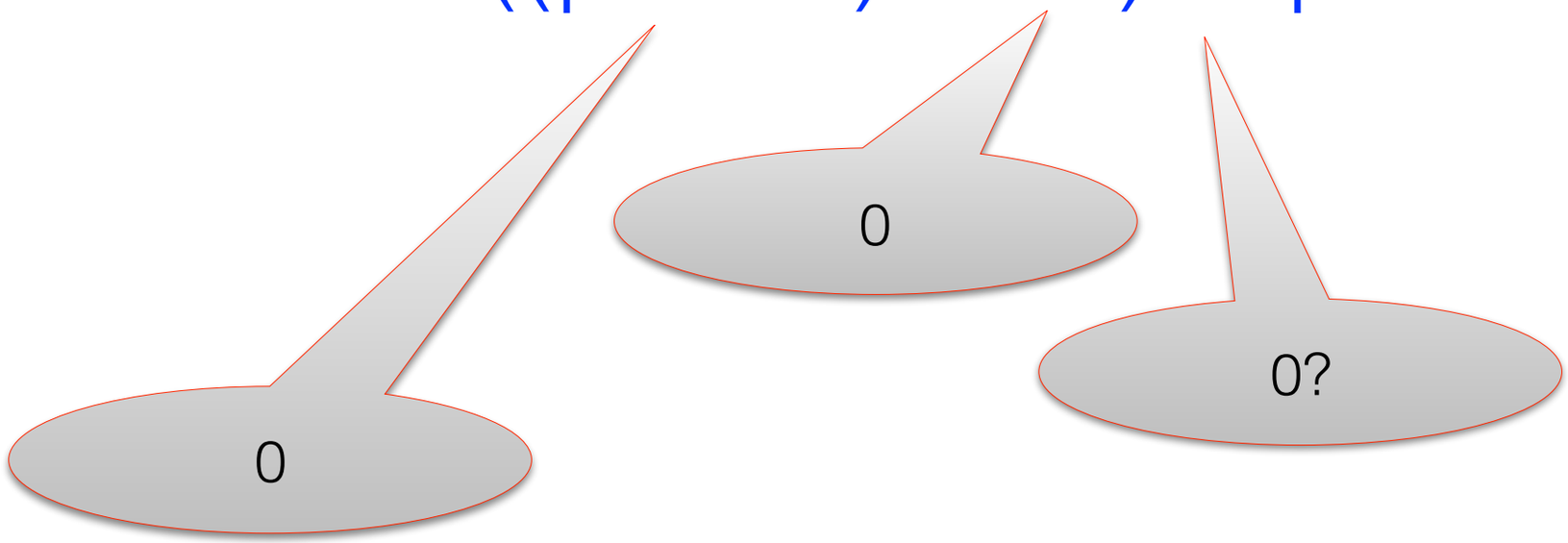


(p -> (p -> **F**)) -> **F**

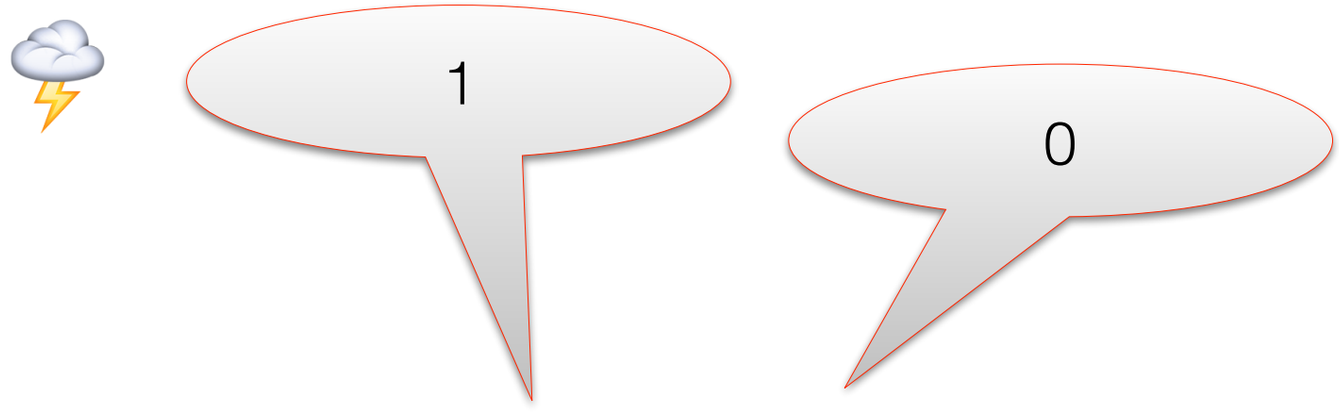
double negation



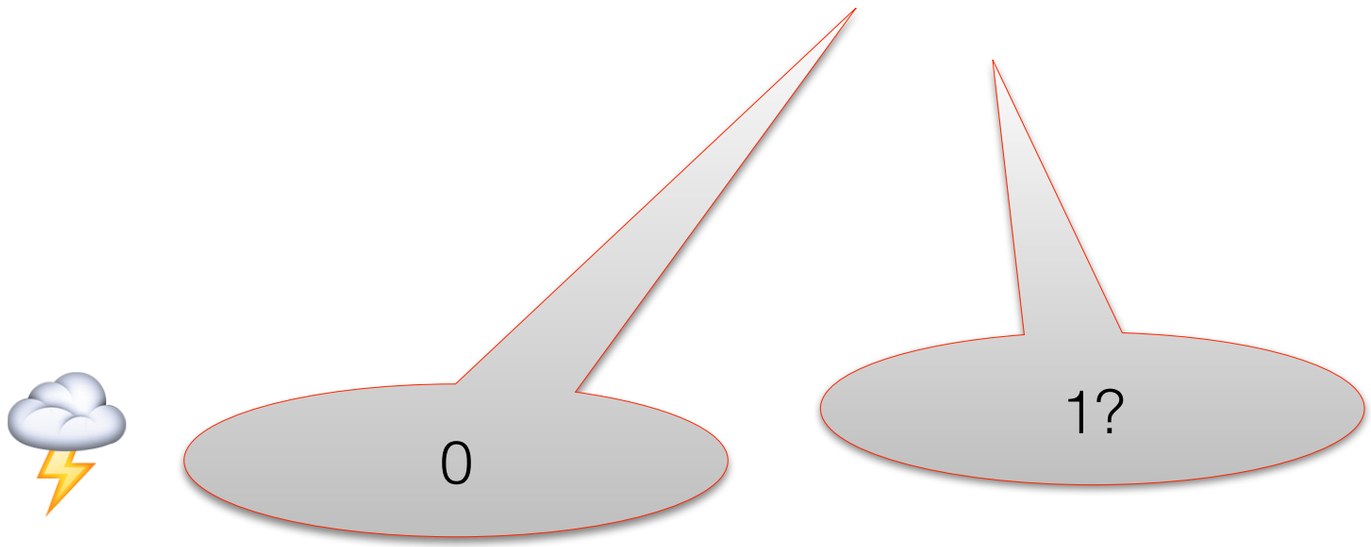
((p -> **F**) -> **F**) ->p



excluded middle



p \/ (p -> **F**)



do we really believe these?

- let us start with a not-entirely-serious example. A lousy use of excluded middle in a work of art:

- *all happy families are alike;*
  each unhappy family is unhappy in its own way

- is this supposed to cover all families?

- how about *not unhappy* ones, which I believe to be the majority? are all not unhappy families alike?

- maybe there is only one path to real happiness (really?). But is there only one way to avoid being unquestionably miserable?

- (and wrt MV/fuzzy approach: how would you measure or put a rational/real value, percentage etc. on *degree of happiness* here?)

- another example: a debate between polticians.
  Let us call them Athos, Porthos and Aramis

- Athos: *I'm not claiming that Aramis is a dishonest person*

- Porthos: *You are convinced then that he is an honest person?*

- Athos: *I've never claimed that either.*

- quite likely, Athos is just implying that there is not enough evidence which would stand in a court of law against cunning lawyers

- (and also bribed/terrorized/biased witnesses, bought/biased media, uncooperative prosecutors etc., but let us disregard here the issue of evidence itself being destroyed, ignored or fabricated—even if this happens all the time)

- compare with:
- Aramis: *Athos is not an honest person*.
- Porthos: *Athos is an honest person*.
- Aramis: *You accuse me of making a false claim, then*?
- Porthos: *Absolutely*.
- Clearly, the status of p -> ¬¬p is very different than ¬¬p -> p

the central idea of intuitionistic and, more generally, constructive approaches to logic:

set up your logical system focusing on evidence rather than truth value

- constructive approach to logical connectives: the Brouwer-Heyting-Kolmogorov (BHK) interpretation

- didactically useful (?) presentation of constructions: prover-skeptic dialogues (Lorenzen, Lorenz, Felscher …)

- elegant natural deduction and sequent-style proof calculi (Gentzen)

- philosophically clean type-theoretical foundation distinguishing judgements and propositions (Martin-Löf)

- usable possible-world semantics: (Kripke, also Beth)

- convenient “externalist/explicitist” perspective via the modal system S4 (Gödel, McKinsey, Tarski)

more things in the vicinity

- computational interpretation (Curry, Howard)
- proof semantics in terms of arbitrary categories (Lambek, Isbell)
- generalization of Kripke-Beth semantics in terms of toposes (Mitchell, Benabou, Joyal)
- closely related systems (Medvedev's of finite problems, Kleene's logic of realizability, Johansson's minimal logic, inquisitive logic, substructural logics…)

a word of warning

- original intuitionism of Brouwer rejected any claim of foundational character of logic

- in fact, Brouwer himself is said to appreciate Boolean algebra as a purely formal system

- on the contrary, doubtful he would agree that IPC (or any formal system) captures the essence of his thought: for him, mathematics was independent not just of outside world or language, but also of logic

- Brouwer's intuitionism nearly extinct in the wild - Dutch government should treat it as protected species!

- since the second half of XXth century, growing alliance between constructivism and formalism

second warning

- excluded middle is rejected in IPC because it doesn't hold for *some* propositions

- if we restrict our attention to well-behaved sentences (e.g., equational sentences of primitive recursive arithmetic: Curry-Goodstein), adding excluded middle would be totally harmless

- in type theory, one speaks of decidable types or types with decidable equality. The name is misleading, if you know what decidability is in general!

bhk

- Brouwer (1908, 1924), Heyting (1934), Kolmogorov (1932)
- a cup that can be filled with differing varieties of wine
- meaning of a statement explained by its construction: what constitutes its proof?
- Kolmogorov spoke of problems rather than propositions

- a proof/construction of P /\ Q is a pair <a, b> where a is a proof/construction of P and b is a proof of Q.

- a proof/construction of P \/ Q is either

  - a pair <a, b> where a is *left* and b is a proof/construction of P, or

  - a is *right* and b is a proof/construction of Q.

- a proof/construction of P -> Q is a **method/function** f that converts a proof/construction of P into one for Q.

- ¬P is defined as P -> **F**, so its proof/construction is a **method/function** converting a proof/construction of P into one for **F** but …

- there is no proof of **F** (the absurdity)

some obvious points

- what's the proof/construction of p \/ ¬p … ??
- but, more importantly, what's *method/function* ?!
- Kolmogorov himself claimed his *problem* reading can be successfully interpreted in a classical setting
- it can be reduced to classical logic, if you interpret all the notions in extensional, set-theoretical way
- (a point M. Escardo likes to make)

back to dialogues?

- perhaps more serious ones than those between Athos, Porthos and Aramis

- presenting them fully correctly in full detail for full IPC surprisingly non-trivial though (Felscher)

- I will follow the example of Sørensen&Urzyczyn and stick to the implicational setting: i.e., with -> the only binary connective

- notation 1: A -> (B -> C) is written as A -> B -> C

- notation 2: let's write x for a formula which is either an atom p, the constant **T** or the constant **F**

- with this convention, every implicational formula is of the form A1 -> A2 -> … -> An -> x, with n possibly equal to 0

- Moreover, if Γ = {A1 … An}, we can define Γ -> B as A1 -> A2 -> … -> An -> B

- before defining formally these dialogues, let us look at the examples first

- Prover: (p -> q -> r) -> (p -> q) -> p -> r !
- Skeptic: fine, here you have your A1: p -> q -> r, your A2: p -> q and your A3: p. How do you get to r?
- Prover: you just told me in A1 I can get to r if I have p together with q
- Ending 1: Skeptic asks where p comes from. Prover: you gave it to me in A3, game over!
- Ending 2: Skeptic asks where q comes from. Prover: in A2, you told me I can get it from p. The dialogue continues as in Ending 1.
- Clearly, Prover has a strategy to kill the Skeptic. Note previous “offers” by Skeptic can be used later!
- Those of you who worked with a proof assistant will find the pattern familiar
- Contrast it with another example …

- Prover: ((p -> q) -> p) -> p !

- Skeptic: fine, here you have your A1: (p -> q) -> p. How do you get to p?

- Prover: you just told me in A1 I can get to p if I have p -> q

- Skeptic: fine, here you have your A2: p. How do you get to q?

- ??? The only way for Prover would be to play tricks — or, as I see it, to cheat. ``Wait, wait, p was what you originally asked me to give. It turns out you had it all the time!''

extending to negation/falsity

- Prover: p -> ¬p -> q!
- Skeptic: fine, here you have your A1: p and your A2: ¬p. How do you get to q?
- Prover: you just check-and-mated yourself. By applying A2 to A1, I get **F**: game over!
- Now try to find a similar proof for ¬¬p -> p…

dialogues, formally

- A dialogue over A: a finite or infinite sequence
  ({A},**T**)! (Σ0,x0)? (Γ1,x'0)! (Σ1,x1)? (Γ2,x'1)! (Σ2,x2)? … where:
- A = Σ0 -> x0 (Skeptic questions the original formula)
- x'n ∈ {xn, F} (Prover meets the challenge or aborts it)
- Γn+1 -> x'n ∈ Σ0 ∪ … ∪ Σn (Prover uses an available offer, also including ones made earlier)
- (Σn,xn) ∈ Γn (Skeptic challenges one of present assumptions)
- Prover wins a play of the game if it reaches the stage with empty Γn (in response to Skeptic's challenge, there was a previously offered atom and there's nothing more to question). Also, if Skeptic poses (Σn,**T**)? as a challenge at some point
- Skeptic wins a play in all the other cases, including ones which simply go on forever
- An implicational formula is provable if there is a winning strategy for the Prover in all dialogues over it

- the two next items I promised were:

- an elegant *natural deduction* proof calculus (Gentzen)

- philosophically clean type-theoretical foundation distinguishing judgements and propositions (Martin-Löf)

- (btw, “judgements”: another vaguely Kantian tune heard in the distance …)

- let’s get them done in one package!

- a nice presentation in *A Judgmental Reconstruction of Modal Logic* by Pfenning and Davies… where you even get to see how to obtain an intuitionistic modal logic this way

- Martin-Löf: *The meaning of a proposition is determined by … what counts as a verification of it*.

- let's use Frege's notation |- A for "A is judged to be true"

- furthermore, let us not restrict the attention to absolute judgements like this (we could only give meaning to /\, but not to -> and even not quite to \/ then)

- hypothetical judgement A1, …, An |- B
  "B is judged to be true assuming A1, …, An are"

- explanation of the meaning of connectives will set up a proof calculus (with nice properties!) allowing to make inferences between hypothetical judgements

- how do we get to A1, …, An |- B /\ C ?

- we need to get A1, …, An |- B and A1, …, An |- C !

- Gentzen's introduction rule for conjunction:

$$\frac{A_1, \ldots, A_n \vdash B \qquad A_1, \ldots, A_n \vdash C}{A_1, \ldots, A_n \vdash B \wedge C}$$

- But, conversely, how we can use or destruct the information encoded in B /\ C ?

- Gentzen's two elimination rules:

$$\frac{A_1, \ldots, A_n \vdash B \wedge C}{A_1, \ldots, A_n \vdash B} \qquad \frac{A_1, \ldots, A_n \vdash B \wedge C}{A_1, \ldots, A_n \vdash C}$$

- taken together, these rules are locally sound (Martin-Löf, Pfenning and Davies):

- one can introduce and then immediately eliminate a connective without losing any information or changing the state of the proof

- btw, some of you may wonder why I'm using notation which feels like sequent system rather than ND. Notation is inessential. The only meaningful difference between sequents and ND are: the former introduce connectives on both sides of |- and aim for cut-elimination, the latter introduce/eliminate on the right side and aim for normalization

implication

- its introduction rule is where we see real use of hypothetical judgements:

$$\frac{A_1, \ldots, A_n, B \vdash C}{A_1, \ldots, A_n \vdash B \to C}$$

- … its elimination is good old Modus Ponens!

$$\frac{A_1, \ldots, A_n \vdash B \to C \qquad A_1, \ldots, A_n \vdash B}{A_1, \ldots, A_n \vdash C}$$

- local soundness embodies function application, but we're skipping Curry-Howard aspects today …

disjunction

- mirrors conjunction … to an extent:

- Gentzen's two introduction rules:

$$\frac{A_1, \ldots, A_n \vdash B}{A_1, \ldots, A_n \vdash B \vee C} \qquad \frac{A_1, \ldots, A_n \vdash C}{A_1, \ldots, A_n \vdash B \vee C}$$

- elimination rule:

$$\frac{A_1, \ldots, A_n, \vdash B \vee C \quad A_1, \ldots, A_n, B \vdash D \quad A_1, \ldots, A_n, C \vdash D}{A_1, \ldots, A_n \vdash D}$$

- even some proof theorists like Girard do not believe it's beautiful! But perfectly meaningful computationally: embodies the `case` construct

falsity

- there is no introduction for falsity (hopefully!)
- its elimination embodies ex falso quodlibet a.k.a. Principle of Explosion:

  $$\frac{A1, \ldots, An \vdash \mathbf{F}}{A1, \ldots, An \vdash B}$$

- (recall the right to abort the challenge in dialogues?)

truth

- there is no elimination rule for **T** : it's useless as a piece of information

- its introduction rule is an axiom (a rule with empty premise): A1 … An |- **T**

- (recall posing it as a challenge resulted in an immediate win by Prover?)

perhaps some whiteboard proofs … if we have the time at this stage

- the next step: encoding proofs by means of proof terms… which correspond to type inhabitants/program expressions

- then we have to think what to do with quantifiers/infinite products/dependent types …

- … and then we have to think what to do with **equality**

- note: no way to justify the Double Negation Law and suchlike without destroying the nice partnership between introduction and elimination rules embodied in principles like local soundness

- this doesn't mean classical calculus doesn't allow ND systems

- but to do it cleanly, one needs to enforce full symmetry between the left and the right side of |-

- and my feeling is that this in turn works best with sequent systems rather than ND

- for those who care about computations: a very nice presentation in *The Duality of Computation* by Curien and Herbelin

the final two items I promised

- usable possible-world semantics: (Kripke, also Beth)
- convenient "externalist/explicitist" perspective via the modal system S4 (Gödel, McKinsey, Tarski)
- assuming there's time, we have to finish this on the whiteboard
- it's also something most participants are likely to have seen before

intuitive motivation

- (following Troelstra)
- both Beth and Kripke based on partially ordered sets
- Beth: possible states of information in time
- Kripke: possible stages of knowledge (less tightly connected to time flow)