Three lightings of logic

Jean-Yves Girard

CNRS, Institut de Mathématiques de Luminy
UMR 6206, 163 Avenue de Luminy, Case 907, 13288 Marseille Cedex 09, France
girard@iml.univ-mrs.fr

Abstract

Whether we deal with foundations or computation, logic relates questions and answers, typically formulas and proofs: a very entangled relation due to the abuse of *presuppositions*.

In order to analyse syntax, we should step out from language, which is quite impossible. However, it is enough to step out from *meaning*: this is why our first lighting of logic is that of *answers*: it is possible to deal with them as meaningless artifacts assuming two basic states, *implicit* and *explicit*. The process of *explicitation* (a.k.a. normalisation, execution), which aims at making explicit what is only implicit, is fundamentally hazardous.

The second light is that of *questions* whose choice involves a formatting ensuring the convergence of explicitation, i.e., the existence of "normal forms". This formatting can be seen as the emergence of *meaning*. It is indeed a necessary nuisance; either too laxist or too coercitive, there is no just format. Logic should avoid the pitfall of Prussian, axiomatic, formats by trying to understand which *deontic* dialogue is hidden behind logical restrictions.

The third lighting, *certainty* deals with the adequation between answers and questions: how do we know that an answer actually matches a question? *Apodictic* certainty — beyond a reasonable doubt — is out of reach: we can only hope for *epidictic*, i.e., limited, reasonable, certainty. Under the second light (questions), we see that the format is made of two opposite parts, namely *rights* and *duties*, and that logical deduction relies on a strict balance between these two opposite terms, expressed by the *identity group* "A is A and conversely". The issue of certainty thus becomes the interrogation: "Can we afford the rights of our duties?"

1998 ACM Subject Classification F.4.1 Mathematical Logic

Keywords and phrases Proof theory

Digital Object Identifier 10.4230/LIPIcs.CSL.2013.11

Category Invited Talk

1 First light: what is an answer?

1.1 Implicit vs. explicit

A simple-minded approach to answers would reduce them to something completely explicit, e.g., `yes` or ||| (the number 3 in Cro-Magnon numeration). However, *implicit* answers, those given by programs or proofs, are more interesting, since *portable*. Indeed, the two sorts of answers, implicit and explicit are linked by *explicitation*: the execution of a program (cut-elimination, normalisation) reduces the implicit to the explicit. To sum up, an implicit answer is a program before execution.

Explicit answers form the solid ground for logic, the ultimate reality, which is made possible by the fact that they convey *strictly no meaning*. But how do we reckon that something is explicit? Is explicit what belongs in the realm of *constatation*, i.e., what is *analytic*. On a traditional typing machine, all keys are constative: they can but add

new text, typically the "↲ " key which opens a new line. On a computer, keys can also assume a *performative* function: "↲ " launches programs. The two aspects, constative and performative, are mingled to the point that one easily launches a program by accident. In logic, the constative and performative aspects of implication were mingled in XIX$^{\text{th}}$ century syntax (Axiom + Rules): *Modus Ponens*. The XX$^{\text{th}}$ century reading (sequent calculus) distinguishes carefully between *implication* $\Rightarrow$ which is handled by the constative left introduction and *entailment* $\vdash$ which is handled by the performative cut rule.

The distinction between implicit and explicit is purely subjective: we *decide* that an object is *finished*, i.e., explicit enough for our taste. A cheque is the typical implicit answer: we must cash it, then spend the money, both operations being hazardous. But we can decide — say, it is a cheque of Paul Erdös — to pin it above the desk. In the same way, a program need not be executed: it can be frozen, or opened with a developer. In logic, a cut on A can be replaced with an left introduction of $A \Rightarrow A \vdash$ (or $\vdash A \otimes {\sim}A$)[1]. This shows that there is no real distinction between, say, programs and data: they all belong to the same analytic space in which explicitation takes place; indeed, the program of explicitation itself must be part of the space.

Although negated by totalitarian ideologies, starting with Bentham's *panoptic* prototype of *Big Brother*, the distinction between implicit and explicit is basic and incompressible. The first evidence is to be found in *incompleteness*: there are questions without answers, typically the Gödel sentence. This evidence is however bridled by the iron discipline of formal systems; we should concentrate on all means of producing explicit answers, including those proscribed by logic. In this lax context, Turing's *undecidability* yields a partial recursive function that cannot be extended into a total one, thus forbidding us to foretell the convergence of execution, i.e., explicitation. By the way, computational complexity deals with a less brutal approach to the distinction between implicit and explicit: some answers are more implicit (harder to compute) than others.

Almost anything can serve as analytic space, for instance the binary integers used in machine code. However, in view of the necessary relation to be made with questions, some choices are more interesting than others. In particular, explicitation should be as natural as possible, so that implicit answers look as much as possible as as *their own execution* — and not as data to which an external program is applied.

A good candidate for an analytic space remains pure λ-calculus; among its good properties, Church-Rosser which states that the implicit contents, if any, is unique. The rewriting style (basically one equation), although external, remains very natural. The limitations are those of the functional paradigm with no direct access to other types of data, e.g., pairs. Also, the treatment of bound variables (α-conversion, substitution) is particularily *ad hoc*. λ-calculus is indeed already too formated: the only abnormality is that of a never-ending normalisation. The absence of deadlocks in pure λ-calculus is both a measure of its intrinsic qualities and of its limitations as an analytic space: deadlocks do exist!

Experience, that of linear logic and parallel computation, compels us to find a more primitive notion, free from functionality, but still deterministic. The various versions of *Geometry of Interaction* eventually stabilised into an analytic space based upon Herbrand's technique of *unification*, which is more primitive, less *ad hoc*, than rewriting: execution can be seen as a sort of physical plugging. This was, by the way, the strongest point in the late *Logic Programming*.

---

[1] This remark can, surprinsingly, be traced back to Lewis Carroll who made a mess of it.

1.2 Stars and galaxies

1.2.1 Unification

Consider a term language with infinitely many functional symbols of each arity. An equation $t = u$ between terms can be solved by means of *substitutions*: t, u are *unifiable* when $t\theta = u\theta$ for some *unifier* θ. The point is that substitutions do compose, hence:

▶ Theorem 1 (Herbrand, 1930). If t, u are unifiable, there is a mother θ_0 of all unifiers for t, u: any unifier θ for t, u can be uniquely written $\theta_0\theta'$.

1.2.2 Flows

A *flow* is an expression $t \leftharpoonup t'$ where t, t' are terms with quite the same variables. These common variables are internal to the flow, in other terms *bound*. In particular, when combining two flows, one must always rename the variables so as to make them distinct. Composition between $t \leftharpoonup t'$ and $u \leftharpoonup u'$ is obtained by *matching* t' and u: matching is the particular case of unification where the terms have no variable in common, what is the case when the variables of t', u have been made distinct. If θ is the principal unifier, we define composition by $(t \leftharpoonup t')(u \leftharpoonup u') := t\theta \leftharpoonup u'\theta$. Composition is thus a partial operation; if we formally add an empty flow 0 to take care of a possible failure of the matching: $(t \leftharpoonup t')(u \leftharpoonup u') := 0$, composition becomes associative, with neutral $I := x \leftharpoonup x$.

If $\mathcal{T}$ is the set of closed terms, then any functional term t induces a subset $[t] \subset \mathcal{T}$, namely the set of all closed t_0 which unify with t; t, t' are *disjoint* when $[t] \cap [t'] = \emptyset$. Any flow $t \leftharpoonup t'$ induces a partial bijection $[t \leftharpoonup t']$ between the subsets $[t']$ and $[t]$ of $\mathcal{T}$. Let us fix a copnstant c; if t_0 is closed, then $[t \leftharpoonup t']t_0$ is defined when $(t \leftharpoonup t')(t_0 \leftharpoonup c) \neq 0$, in case it writes $[t \leftharpoonup t']t_0 \leftharpoonup c$. The condition "quite the same variables" ensures that $[t \leftharpoonup t']t_0$ is closed and that $[t \leftharpoonup t']$ is injective. Any flow $u \leftharpoonup u$ is idempotent; its associated function is the identity of the subset $[u] \subset \mathcal{T}$.

1.2.3 The convolution algebra

One can introduce the *convolution algebra* of the monoid, i.e., the set of finite formal sums $\sum \lambda_i \phi_i$ where the ϕ_i are flows and the λ_i are complex coefficients, the improper flow 0 being identified with the empty sum. This algebra acts on the Hilbert space $\ell^2(\mathcal{T})$ by means of $(t \leftharpoonup t')(\sum_i \lambda_i t_i) := \sum_i \lambda_i [t \leftharpoonup t']t_i$. The involution $(\sum \lambda_i (t_i \leftharpoonup t_i'))^* := \sum \bar{\lambda}_i (t_i' \leftharpoonup t_i)$ is implemented by the usual adjunction. The idempotents $t \leftharpoonup t$ correspond to the projections on the subspaces $\ell^2([t])$ and $t \leftharpoonup t'$ induces a partial isometry of *source* $\ell^2([t'])$ and *target* $\ell^2([t])$. The early versions of GoI did associate to proofs finite sums of flows. These sums were *partial isometries*; $u = \sum t_i \leftharpoonup t_i'$ is a partial isometry (i.e., $uu^*u = u$) if the targets t_i are pairwise *disjoint*, not unifiable, *idem* for the t_i'. The operators of GoI are indeed *partial symmetries* ($u = u^3 = u^*$): typically the identity axioms $(t \leftharpoonup t') + (t' \leftharpoonup t)$ (t, t' disjoint).

The unification algebra internalises the major algebraic constructions.

Matrixes

If I is a finite set of closed terms, the $I \times I$ matrix (λ_{ij}) can be naturally represented by $\sum_{ij} \lambda_{ij} (i \leftharpoonup j)$.

Direct sums

The flows $P := p(x) \leftharpoonup x, Q := q(x) \leftharpoonup x$ induce an isometric embedding of $\ell^2(\mathcal{T}) \oplus \ell^2(\mathcal{T})$ in $\ell^2(\mathcal{T})$: $x \oplus y \mapsto [P]x + [Q]y$. The isometricity comes from $P^*P = Q^*Q = I$, $P^*Q = Q^*P = 0$. The embedding is not surjective: this would require $PP^* + QQ^* = I$, in other terms that every term matches either $p(x)$ or $q(x)$.

P and Q have been heavily used in the early GoI, in particular for multiplicatives — and, modulo tensorisation with I, for contraction. They enable one to change the size of matrices in a flexible way. Usually, the only possibility is to *divide* the size, typically $\mathcal{M}_{mn}(\mathbb{C}) \simeq \mathcal{M}_m(\mathcal{M}_n(\mathbb{C}))$ replaces a $mn \times mn$ matrix with a $m \times m$ matrix whose entries are $n \times n$ matrices, i.e., blocks of size $n \times n$. Thanks to P, Q, one can replace a 3×3 matrix with a 2×2 one (with four "blocks" of sizes $2 \times 2, 2 \times 1, 1 \times 2, 1 \times 1$).

Tensor products

The tensor product of two flows makes use of a binary function "$\cdot$" and is defined by $(t \leftharpoonup t') \otimes (u \leftharpoonup u') := t \cdot u \leftharpoonup t' \cdot u'$; the variables of the two flows must first be made distinct. This corresponds to an internalisation of the tensor product, which plays an essential role in the handling of exponentials, i.e., of repetition. The flow $T := (x \cdot y) \cdot z \leftharpoonup x \cdot (y \cdot z)$ compensates the want of associativity of the internal tensor: $T^*(((t \leftharpoonup t') \otimes (u \leftharpoonup u')) \otimes (v \leftharpoonup v'))T = (t \leftharpoonup t') \otimes ((u \leftharpoonup u') \otimes (v \leftharpoonup v'))$.

Crown products

In the same style as T, the flow
$\sigma := x_1 \cdot (x_2 \cdot (\dots (x_{n-1} \cdot x_n) \dots)) \leftharpoonup x_{\sigma(1)} \cdot (x_{\sigma(2)} \cdot (\dots (x_{\sigma(n-1)} \cdot x_{\sigma(n)}) \dots))$ induces a permutation of the constituents af a n-ary tensor.

1.3 Stars and galaxies

1.3.1 Stars

A *star* $[\![t_1, \dots, t_{n+1}]\!]$ consists in $n+1$ terms; these terms, the *rays* of the star, must be pairwise *disjoint*, i.e., not matchable, which is strictly stronger than *not unifiable*.

Stars generalise the unification algebra; thus, the axiom link $(t \leftharpoonup t') + (t' \leftharpoonup t)$ becomes $[\![t, t']\!]$. However, since our objects are no longer operators, there are some difficulties in defining the analogue of composition. For this we shall use *coloured stars*. We select pairs of complementary colours, e.g., (`green`, `magenta`) together with the *neutral* colour `black`; a *coloured star* is a star in which each ray has been given a colour: typically, $[\![t, u, v, w]\!]$. Disjointness is required only for rays of the same colour, which comes from the fact that coloured stars are not yet another notion, just a shorthand: indeed, consider three unary functions g, m, b and replace $[\![t, u, v, w]\!]$ with $[\![g(t), g(u), b(v), m(w)]\!]$. t is thus *a priori* disjoint from u.

1.3.2 Galaxies

A *galaxy* is a finite set of coloured stars. Cut-free proofs will be represented by black galaxies, whereas the cut-rule will make use of complementary colours. The implicit thus lies in the use of colours, this explains why it is relative and contextual: by making everything black, a galaxy becomes explicit at no cost. Colours thus indicate that we consider the data as unfinished, thus initiating a *normalisation* process.

In order to normalise a galaxy, we first form its *diagrams*. By this I mean any tree (in the topological acception) obtained by attaching $N+1$ stars of the galaxy by means of N *vertices*. By a *vertex*, I mean a pair $t = u$ of rays of complementary colours. Since the same star may be used several times in a diagram, a galaxy is likely to generate infinitely many diagrams.

The *unification* of a diagram consists in unifying its vertices, so that $t\theta = u\theta$ becomes an actual equality. Most unifications will fail; we are basically concerned with *correct* diagrams, those for which unification succeeds.

1.3.3 Normalisation

In usual GoI, the cut-rule is handled by a partial symmetry σ; the normal form of the proof (u, σ) is given by:

$$(I - \sigma^2)u(I - \sigma u)^{-1}(I - \sigma^2)$$

Here σ corresponds to the swapping of complementary colours: σ exchanges `green` and `magenta` and "kills" `black`. Under reasonable hypotheses (nilpotency), $u(I - \sigma u)^{-1}$ can be written as a finite sum $u + u\sigma u + u\sigma u\sigma u + \ldots$, which corresponds to the plugging of u with itself through complementary colours. The two $I - \sigma^2$ correspond to the restriction to the "black stars".

Strong normalisation) generalise the nilpotency of σu:

1. There are only finitely many correct diagrams. In other terms, for an appropriate N, all diagrams of size $N+1$ fail; this finite N accounts for *strong* normalisation.
2. No correct diagram is *closed*, i.e., without a free ray. The condition thus excludes the closed diagram $\{[\![\, t \,]\!], [\![\, t \,]\!]\}$ (vertex $t = t$).
3. In a correct diagram, identify complementary colours, e.g., replace `magenta` with `green`; then the free rays are disjoint. The simplest diagram thus excluded consists of a single binary star: $\{[\![\, t, u \,]\!]\}$, with t, u not disjoint.

The normal form is obtained by collecting the correct diagrams whose free rays are black. And to replace them with their *residual* star, i.e., the star whose rays are their free rays.

A galaxy $\mathcal{G}$ is *isometric* when rays of the same colour occurring in $\mathcal{G}$ are pairwise disjoint. The normal form of an isometric galaxy is easily shown to be isometric.

1.3.4 Church-Rosser

In the presence of two pairs of complementary colours, there are three possible ways of normalising:

1. Identify `green` = `blue`, `magenta` = `yellow` and normalise.
2. Normalise the cuts `blue`/`yellow`, then the residual cuts `green`/`magenta`.
3. Normalise the cuts `green`/`magenta`, then the residual cuts `blue`/`yellow`.

The Church-Rosser property equates (in any possible sense) these three possibilities. This property will later be used to show the *compositionality* of cut, hence to develop various functional, i.e., category-theoretic, interpretations. Hence one pair of colours is enough, at least for theoretical considerations.

2 Second light: what is a question?

2.1 Formatted vs. informal

An implicit answer, a program, may have no explicit contents: normalisation may diverge. Fixing that point amounts at *formatting*; the emergence of meaning wholly lies in this formatting. A synonym for meaning is *question*: the meaning of the answer is the question it is supposed to solve. Now, there is a great divide between the formatted, typed, logical approach and the unformal, untyped, "free" approach.

The lesson of incompleteness is that the format is a *necessary nuisance*, think of Family, Justice, Police, etc. Indeed, the informal approach to logic is inconsistant — if we prefer, the untyped approach to computation does not normalise: this account for the "necessary". On the other hand, a typing discipline always misses something. This remark is already present in Richard's Paradox (1905): "The smallest integer not definable in less than twenty words". The informal acception of "definable" makes it inconsistent, while a formated version — say DEFINABLE — avoids the pitfall while producing a definition out of the scope of "DEFINABLE".

The same totalitarian ideologies that claim that everything is explicit, transparent, would consistently vouch for informality: witness the various *qualunquists* (libertarians, populists, etc.) which pretend to approach politics without politicians, taxes, laws. When in charge, these people turn out to be worse than the politicians they were opposing to. This is due the fact that one cannot escape formatting: and then, better an explicit than a hidden one!

The real question is thus not that of the necessity of a format, but that of its nature, its emergence. XIX$^{\text{th}}$ logic solved the problem by means of *axiomatics*, i.e., principles that one cannot discuss. There must be something of the like, but we should at least understand what we accept: axiomatics is too Prussian to be honest[2]. In logic, the format is usually invisible; besides the choice of a language to avoid inconsistencies, it also occurs in the *form* preserved by category-theoretic *morphisms* or in the *rule* of game-theoretic semantics. Can we discuss these choices, or better: is this discussion part of logic?

The situation of an opaque *deontic*, normative[3], kernel did not change till the invention of *linear logic* in the mid eighties. Indeed, the existing formats, especially *natural deduction*, were satisfactory enough to make us forget their axiomatic, Prussian, character. Linear logic, with the introduction of classical features — basically an involutive negation — within the constructive universe, posed a novel question, namely the handling of several simultaneous conclusions, a problem hitherto avoided by the tree-like format which pinpoints both the conclusion and the last rule applied. In *proof-nets*, the last rule is implicit to the point that it is not even uniquely defined. What makes a proof-net correct, i.e., what compels it to have a last rule and, this recursively, is a purely deontic question.

The question was not quite novel, since Herbrand's theorem solved it in the limited context of quantification. In a prenex form, the existentials should be given as functions $y_i = t[x_1, \ldots, x_n]$ of the universals. Assuming we forgot the step-by-step construction of t, Herbrand replaces x with $f(y)$ in the case of a formula $\exists y \forall x$; if x actually occurs in t, then we get a cycle (failed unification) $y = t[f(y)]$.

The sort of dialogue at work in Herbrand's theorem — more generally in proof-nets — is not basically designed to tell truth from falsity, but what is permitted from what is illegal. This dialogue is *deontic* (instead of *alethic*): it deals with permissions, obligations, and not with

[2] In modern Greek, *axiomatikos* means "officer"!
[3] This adjective may convey a derogatory approach to the format; "deontic" is more neutral.

truth. A typical deontic dialogue is "Objection your Honor! Objection sustained/overruled". The dialogue has nothing to do with the truth/falsity of the statement under discussion: it concerns its relevance to the case. One perfectly understands that not every question should be taken into consideration; but also that this necessary deontic dialogue may be a way to sweep things under the carpet.

Popper's notion of *falsifiablity* is a limited form of deontic dialogue accounting for purely universal, Π^0_1, formulas of arithmetic, e.g., $\forall x\ (x+1)^2 = x^2 + 2x + 1$. Falsifiability does not hold beyond Π^0_1 complexity, for the simple reason that falsifiability is itself Π^0_1: "for all tests…". Beyond the Π^0_1 case, the deontic dialogues becomes completely symmetric: if an objection is overruled, something goes wrong, but we cannot foretell which side "is right": when the judge says "sustained", he may be dismissed!

2.2 Vehicles and gabarits

We restrict our presentation to the familiar multiplicative case of linear logic.

2.2.1 Proof-nets

We should get rid of syntactical decorations so as to describe multiplicative proof-nets in a purely *locative* way: in order to represent a proof of $\vdash A, B, C$ unary functions p_A, p_B, p_C will be used to distinguish between the various *locations* available in the sequent; I could as well use p_1, p_2, p_3, but this would compel me into a systematic reindexing.

2.2.2 Vehicles: cut-free case

Let us choose, once for all, distinct constants $\mathtt{l}, \mathtt{r}$ and a binary function letter "$\cdot$". To each proof π we associate its *vehicle*, i.e., a galaxy $\pi^\bullet$; this galaxy is black in the cut-free case.

Identity axiom: if π is the axiom $\vdash A, {\sim}A$, then $\pi^\bullet := \{[\![\, p_A(x), p_{\sim A}(x) \,]\!]\}$.

$\parr$-rule: if the proof π of $\vdash \Gamma, A \parr B$ has been obtained from a proof ν of $\vdash \Gamma, A, B$, then $\pi^\bullet := \nu^\bullet$ in which p_A and p_B are now *defined* by
$p_A(x) := p_{A\otimes B}(\mathtt{l}\cdot x)$, $p_B(x) := p_{A\otimes B}(\mathtt{r}\cdot x)$.

$\otimes$-rule: if the proof π of $\vdash \Gamma, A \otimes B$ has been obtained from proofs ν of $\vdash \Gamma, A$ and μ of $\vdash B, \Delta$, then $\pi^\bullet := \nu^\bullet \cup \mu^\bullet$, with p_A, p_B *defined* by
$p_A(x) := p_{A\parr B}(\mathtt{l}\cdot x)$, $p_B(x) := p_{A\parr B}(\mathtt{r}\cdot x)$.

The vehicle is thus a galaxy of axiom-links, seen as stars. The rules $\parr, \otimes$ have been used to relocate these links. For instance, the axiom $[\![\, p_A(x), p_{\sim A}(x) \,]\!]$ may relocate as $[\![\, p_{A\parr(\sim A\otimes B)}(\mathtt{l}\cdot x), p_{A\parr(\sim A\otimes B)}(\mathtt{r}\cdot(\mathtt{l}\cdot x)) \,]\!]$.

2.2.3 Vehicles: general case

In presence of cuts, coloured functions will be needed. We shall use a pair of complementary colours, typically $p_B, p_{\sim B}$ and $p_B, p_{\sim B}$. The interpretation $\pi^\bullet$ now looks as a union $\mathcal{V} \cup \mathcal{C}$: $\mathcal{V}$ (in black and `green`) is the vehicle proper, $\mathcal{C}$ — its *feedback* — is easily identified as the `magenta` part of the vehicle.

Cut rule: if the proof π of $\vdash \Gamma$ has been obtained from proofs ν of $\vdash \Gamma, A$ and μ of $\vdash {\sim}A, \Delta$, then $\pi^\bullet := \nu^\bullet \cup \mu^\bullet \cup \{[\![\, p_A(x), p_{\sim A}(x) \,]\!]\}$; furthermore, in $\nu^\bullet \cup \mu^\bullet$, $p_A, p_{\sim A}$ have been painted `green`: $p_A(t) \mapsto p_A(t)$, $p_{\sim A}(t) \mapsto p_{\sim A}(t)$.

2.2.4 Gabarits (I)

We must now make sense of the lower part of the proof-net, the one dealing with the $⅋, \otimes$ and Cut links. The main problem is to give a precise definition of the switching discipline leading to the correctness condition. Indeed, to each switch, we shall associate an *ordeal*, i.e., a coloured galaxy. This finite set of ordeals is called the *gabarit*.

We already defined the unary functions $p_A(x)$ for each formula and subformula of the proof-net. We now introduce $q_A(x) := p_A(\mathtt{g} \cdot x)$, where $\mathtt{g}$ is yet another constant. The replacement of p_A with q_A in the context of gabarits is due to the fact that $p_{A\otimes B}(x)$ is not disjoint from $p_A(x) := p_{A\otimes B}(\mathtt{l} \cdot x)$, whereas $q_{A\otimes B}(x)$ and $q_A(x)$ are disjoint: the q_A provide disjoint locations for the formulas occurring in the lower part of the proof-net.

Given a proof-net of conclusions Γ, a switch L/R of its $⅋$-links induces an *ordeal*, namely the coloured galaxy made of the following stars:
$\boldsymbol{X, \sim X}$: $[\![\, p_A(x), q_A(x) \,]\!]$ when A is a *literal* $X, Y, \sim X, \sim Y, \ldots$.
$\otimes$: $[\![\, q_{A\otimes B}(x), q_A(x), q_B(x) \,]\!]$.
$⅋_L$: $[\![\, q_{A⅋B}(x), q_A(x) \,]\!]$ and $[\![\, q_B(x) \,]\!]$. In terms of graphs, $[\![\, q_B(x) \,]\!]$ "terminates" all $[\![\, q_B(t) \,]\!]$.
$⅋_R$: $[\![\, q_{A⅋B}(x), q_B(x) \,]\!]$ and $[\![\, q_A(x) \,]\!]$ which "terminates" all $[\![\, q_A(t) \,]\!]$.
Cut: $[\![\, q_A(x), q_{\sim A}(x) \,]\!]$.
Conclusion: $[\![\, q_A(x), p_A(x) \,]\!]$ when $A \in \Gamma$, i.e., is a conclusion.
An ordeal thus normalises into a galaxy in `black` (conclusions) and `blue` (literals).

2.2.5 Correctness, a.k.a. completeness

Let $\mathcal{V}$ be $\mathcal{V}$ painted `yellow`. The *correctness criterion* thus writes as:

> For any ordeal $\mathcal{S}$, the galaxy $\mathcal{V} \cup \mathcal{S}$ strongly normalises into $\{[\![\, p_A(x) \;;\; A \in \Gamma \,]\!]\}$.

This condition is obviously necessary; its sufficiency is the most elaborate form of *completeness* that one can imagine, since it relates the symbolic testing by means of the ordeals with the proofs in a logical system.

The main technical problem with completeness is that usual proof-nets are, so to speak, "preconstrained": the identity links relate complementary formulas $A, \sim A$, whereas nothing of the kind has been so far required. In other terms, our treatment of literals is completely indistinct: $X, \sim X, Y$ are the same, up to their locations. How can we force an axiom link to relate X with a $\sim X$ (and not a Y, nay another X)?

Here, we must remember that predicate or propositional calculi are convenient structures, but that part of them belongs in the worst kind of *a priori*. Typically, the so-called propositional "constants" X, Y and their negations: we are embarrassed since they mean nothing by themselves. The real logic is a second order system — a sort of system $\mathbf{F}$ — in which there is no propositional constants, but in which formulas are *closed*. What we call first order logic indeed corresponds to those formulas $\forall X_1 \ldots \forall X_n A$, with A quantifier-free: the behaviour of such formulas is extremely simple, especially in view of completeness issues, e.g., the subformula property. The restriction to those formulas renders the universal prefix compulsory —hence the possibility to omit it. To make the long story short, when dealing with a proof-net, we must take into account the *implicit* second order quantification $\forall X$ on all propositional "constants". What follows is a glimpse of the future treatment of second order logic; indeed the easy case of the quantifier $\forall X$.

Every propositional "constant" must be switched; each switch has three positions, so that n propositional constants induce 3^n possibilities. The switching corresponds to the choice $\boldsymbol{\Theta}$ of a substitution $X_i \rightsquigarrow \mathbf{c}_i$ for each of the "constants" X_i, the $\mathbf{c}_i$ ranging over the

three possibilities $\mathbf{a}, \mathbf{a} \otimes \mathbf{b}, \mathbf{a} \parr \mathbf{b}$, where $\mathbf{a}, \mathbf{b}$ are propositional letters. Now, to switch our net consists in:

1. First switch the constants, thus yielding a substitution $\mathbf{\Theta}$.
2. Then switch $\mathbf{\Theta}(\Gamma)$ as explained above.

This should be enough to ensure that literals are linked according to the book. As to general axiom links (not between literals) an argument based upon ηxpansion should exclude "illegal" links.

2.2.6 Gabarits (II): virtual switches

Let us turn our attention towards an exotic multiplicative, namely the "linear affine" implication $A \multimap B$. "$\multimap$" yields a purely multiplicative second-order reduction of additives: $A \oplus B := \forall X((A \multimap X) \multimap ((B \multimap X) \multimap X))$[4].

Indeed, $A \multimap B$ is an intuitionistic implication without reuse of premises; this is why it interests us. The associated disjunction $A \ltimes B := {\sim}A \multimap B$ is problematic in terms of gabarits. Indeed, the $\ltimes$-link:

$$\frac{[A] \quad B}{A \ltimes B}$$

is problematic: the premise A (written $[A]$ for this reason[5]) might be absent, hence the switch "L" is hazardous: it may destroy everything in case of absence. On the other hand, we cannot content ourselves with the sole "R", hence the idea of a *virtual switch*, i.e., a sort of compensation for the missing switch.

Virtual switches are inspired from the proof by Mogbil and de Naurois of the NL complexity of multiplicative proof-nets; improving the idea of *contractibility* introduced by Danos, the authors show that it is enough to switch $\parr$ on one side, e.g., always "R"; an additional order condition (3 below) compensates for the missing switches. The point is that this alternative approach can be used in case we cannot switch the $\parr$ on "L", typically if the actual presence of the premise A is dubious. This is the case with the marginal connective $\ltimes$, a multiplicative which *actually* needs virtual switches.

A *virtual switch* is a star $[\![t; u_1, \dots, u_n]\!]$, with a distinguished ray, its *root* t. $u_1, \dots, u_n$ must be pairwise disjoint; each variable occurring in t must still occur in the u_i.

The notion of ordeal is modified as follows, so as to include an auxiliary galaxy of virtual switches. Typically, in the case of $A \ltimes B$, besides $[\![q_{A \ltimes B}(x), q_B(x)]\!]$ and $[\![q_A(x)]\!]$, we add the auxiliary stars $[\![q_{A \ltimes B}(x); q_A(x)]\!]$.

Consider the unique correct diagram in $\mathcal{V} \cup \mathcal{S}$, and let us unify it, so as to get a galaxy $\mathcal{G}$. For each virtual switch $[\![t; u_1, \dots, u_n]\!]$, consider all rays obtained by unification from some u_i; since $u_i\theta = u_i\theta'$ implies $t\theta = t\theta'$, each such ray "comes from" a specific instanciation of t, its "root". We require that:

1. If $u_i\theta \in \mathcal{G}$, then its root $t\theta$ occurs in $\mathcal{G}$.
2. $u_i\theta$ is "upwards connected" to $t\theta$, i.e., the connection does not transit through the vertex $t_1\theta_1 = t\theta$.

[4] Instead of $\forall X((A \multimap X) \Rightarrow ((B \multimap X) \Rightarrow X))$.
[5] The graphism is reminiscent of the discharged hypotheses of natural deduction.

For each $t\theta$ in $\mathcal{G}$, we can consider the set $\mathcal{G}_{t\theta}$ of all rays standing in between $t\theta$ and some $u_i\theta'$ with root $t\theta$ (i.e., s.t. $t\theta = t\theta'$) including extremities; $\mathcal{G}_{t\theta}$ is this a sort of tree, rooted in $t\theta$. We define $t_1\theta_1 \preceq_1 t_2\theta_2$ by $t_1\theta_1 \in \mathcal{G}_{t_2\theta_2}$. If $\preceq$ is the reflexive and transitive closure of $\preceq_1$, we require that:

3. $\preceq$ is an order relation.

These conditions (especially 3) are clearly CO-NL, hence their complexity-theoretic import. To understand how virtual switches work, let us assume that the ordeal $\mathcal{S} \in \mathcal{G}$ switches the $⅋$ link with conclusion $A ⅋ B$ on "R" and that its virtual part contains $[\![q_{A⅋B}(x), q_A(x)]\!]$; we can get rid of this virtual switch by adding to $\mathcal{G}$ the ordeal $\mathcal{S}'$, namely the twin of $\mathcal{S}$ with the same $⅋$ switched on "L": conditions 1 – 3 precisely allow for this replacement. We can thus eliminate the virtual switch $[\![q_{A⅋B}(x), q_A(x)]\!]$ from $\mathcal{G}$ at the price of a duplication of the number of its ordeals.

Virtual switches are well-adapted to weakening, since they cope with the possible uncertainty as to the presence of a specific premise. Moreover, since u_i may contain variables not in t, there is no limitation as to the number of $u_i\theta'$ rooted in a given $t\theta$: the extra variables thus account for contraction. The treatment of exponentials and additives makes a heavy use of virtual switches.

3 Third light: what conveys certainty?

3.1 Epidictic vs. apodictic

The main difference between XIX$^{\text{th}}$ century, pre-Gödelian, and XX$^{\text{th}}$ century logics is perhaps the issue of *certainty*. Before incompleteness, a proof was supposed to be valid beyond any doubt; hence the adjective *apodictic*, which corresponds to this absence of doubt, but whose etymology is simply "proven". Incompleteness opens the possibility of a reasonable doubt, hence to a change of status for proofs: they are no longer apodictic, they can only be *epidictic*, i.e., they only guarantee a reasonable form of certainty. Common sense can explain this failure: deduction is a rational form of prediction, but prediction cannot be 100% rational. Just like rating agencies were unable to prevent the subprime crisis, there is no absolute certainty as to cheques, before cashing. The only absolutely reliable bank is completely explicit: it directly delivers the goods you are looking for, the cow and the butter: but then, forget money! In the same way, the only absolutely reliable formal system would be purely analytic, limited to down to earth constatations of the form $2 + 2 = 4$.

How come that our certainty is no longer that certain? We must remember that it never occurred to XIX$^{\text{th}}$ century logicians, e.g., Russell, Hilbert, that the logical format could "miss" some "truth", unless the definition was intentionally ambiguous. For instance, Euclide's Postulate left open the question of parallels, but this was made explicit by alternative models, the sphere or the one-sheet hyperboloid; this question being fixed, nothing else was "missing". In the case of incompleteness, nothing specific is actually missing in the sense that it would suffice to add it. But there is a definite shortage of counter models: nobody has ever seen the tail of a refutation of the Gödel sentence — the book says that such a refutation must exist — but this "evidence" follows from incompleteness, while it should establish it. This is why this "model" is styled *non standard*, i.e., good for nothing.

Back in the 1920s, the only possibility was that of proving too much, like in Burali-Forti's or Russell's antinomies. Hence the reduction of certainty to *consistency*: if a deductive system cannot prove A and $\neg A$, then it should be perfectly sound, i.e., conveys certainty. However, $\mathbf{PA} + \neg G$, Peano Arithmetic extended with the negation of the Gödel sentence is

equi-consistent with **PA**, although plainly wrong! An analogy: many criminals are found "not guilty" on the grounds of some legal trick, say a statute of limitations; but an acquittal based on a deontic use of Law can by no means restore confidence. In other terms, although the negation $\neg G$ avoids inconsistency, it is still far from plausible: consistency does not entail certainty.

We must however reckon that consistency is (a minor) *part of* certainty. Here the second incompleteness destroys the ultimate illusion of XIX$^{\text{th}}$ century logic: consistency itself cannot be established beyond a reasonable doubt.

Gödel's incompleteness is the final firework of XIX$^{\text{th}}$ logic. XX$^{\text{th}}$ logic begins with Gentzen's cut-elimination (the distinction implicit/explicit), Herbrand's theorem (the emergence of format) and the "functional" interpretation of proofs, a.k.a. BHK[6]. Typically, a proof of $\forall x\ A[x]$ is a function associating to each integer n a proof $f(n)$ of $A[n]$. The definition is interesting and problematic under the three lights:

Answers: f cannot be quite a function, since a function is an infinite object. It must thus be a finite artifact, a program yielding the output $f(n)$ when feeding it with n.

Questions: f must be of the right kind, i.e., associate to each n a proof of $A[n]$, whatever that means. Deontically speaking, this means that f must pass infinitely many tests: first choose n, then test whether $f(n)$ is a proof of $A[n]$. Something of the like occurs with Popper's *falsifiablity*.

Certainty: how do we know that the proof is actually a proof, in other terms, that it passes the deontic tests which are infinetely many? In the Π^0_1 case, this *proof that the proof is a proof* is indeed the proof irself: the function, something like $f(n) := \texttt{true}$ is known in advance, so the only thing at stake is to determine whether $A[n] = \texttt{true}$ for all n, i.e., $\forall x\ A[x]$.

BHK can thus be seen as an archaic prefiguration the most recent developments in terms of answers and questions: in that respect, it fully belongs in XX$^{\text{th}}$ century logic. It also poses the problem of certainty: and, to start with, how come, in XX$^{\text{th}}$ century terms, that we lost absolute certainty?

3.2 Derealism

3.2.1 Proof-nets and certainty

The correctness criterion for proof-nets yields a form of apodictic certainty: yes, we can be sure that a would-be proof is actually a proof. This is due to the combination of several facts:

Finiteness: correction relates a vehicle with a gabarit. This involves finitely many finite verifications, leaving no room for reasonable doubt.

Compositionality: the gabarit for A and the gabarit for $\sim A$ do match so as to ensure the identity group, especially cut-elimination.

The great divide of logic is between first and second order. Indeed, if we take a second order approach to logic (with quantifiers on predicates or propositions), the first order part is the one in which second order quantifiers occur as universal prefixes $\forall X_1 \dots \forall X_n$: the formula $X \Rightarrow X$ is thus a shorthand for $\forall X\,(X \Rightarrow X)$. Using the Dedekind translation of natural numbers, arithmetic becomes part of second order logic: indeed, Π^0_1 formulas involve second order existentials. First order is complete and apodictic, while second order proper — i.e., using $\exists X$ — is incomplete and can only be epidictic.

[6] Indeed Brouwer-Heyting-Kolmogorov.

Something puzzling is that the proof-net technology basically applies to full logic. The fact that we lose certainty must be ascribed to second order quantification, more precisely, to the the existential quantifier. The study of system **F** shows that this quantifier concentrates most of the logical complexity: its interpretation through *candidats de réductibilité* involves comprehension axioms, which cannot convey absolute certainty.

Indeed, in a second-order proof-net, we must indicate the existential witnesses T corresponding to the rules deducing $\exists X\, A[X]$ from $A[T]$. And, relative to these witnesses T (which carry their own gabarits), we can get absolute certainty, at least on the grounds of *finiteness*. The issue of compositionality is, however, a cat of a different colour: indeed, X occurs several times in $A[X]$, in practice both positively and negatively. This means that we must provide gabarits for both T and $\sim T$. But how do we know that they actually match?

We already mentioned, concerning Popper, that his approach was too simplistic: like in the Gospel, the judges must be judged. This means that the matching between the normativity for T and the normativity for $\sim T$ is the most intricate thing one can imagine, surely something not of this world. The reasonable doubts and the reasonable certainties as to reasoning concentrate in this hazardous matching.

3.2.2 Épures

The deontic pair $T/\sim T$ corresponds to the *rights* and *duties* attached to T. The identity axiom $T \vdash T$, or, better, $\vdash \sim T, T$ is still valid when we relinquish our rights — and/or exaggerate our duties. But the cut rule enables to pass from $\vdash \Gamma, T$ and $\vdash \Delta, \sim T$, to $\vdash \Gamma, \Delta$ on the basis that we have the rights (T) of our duties ($\sim T$). By the way, replacing T with $\sim T$ will not alter the pattern, since the rights of $\sim T$ are the duties of T.

This schizophrenic approach to deduction first occurred in Schütte's *partial valuations*, in other terms, three-valued models. The fact that one can relinquish our rights is expressed by a third value, $\boldsymbol{i}$. Hence, in terms of rights, A is not false, while in terms of duties, A is true. The fact that "true" implies "not false" accounts for the identity axiom. But the cut rule requires the reverse implication, which is the case only in the usual, two-valued case. This semantics is, as far as I know, the unique legitimate occurence of an exotic truth value. Its technical interest is almost void: since $\boldsymbol{i} \Rightarrow \boldsymbol{i} = \boldsymbol{i}$, the third value has a propension to swallow the real ones... and what is the use of a model where almost everything takes the value $\boldsymbol{i}$? The only interest of the third value is that of a sort of "side wheels" helping us from mixing rights and duties.

A much better incarnation of the same idea is the category-theoretic notion of *dinaturality*: the entailment $A \vdash A$ between rights and duties becomes a morphism. And the failure of compositionality can be ascribed the want of commutativity of certain "hexagons". But this is still semantics, not yet the real thing.

The French "épure" means the representation of an object through three planar projections. I propose to use this term for the combination $\mathcal{V} + \mathcal{G}$ of a vehicle and a gabarit: indeed, both an object and several ways (the ordeals of $\mathcal{G}$) of structuring it. The inclusion of a gabarit as part of the épure renders quantification over gabarits possible: this should answer for the problematic aspects of second order logic. By the way, if a proof is an épure, the missing "auxiliary proof" of BHK is its gabarit.

3.2.3 The derealistic program

If we except first order quantification and equality, our understanding of first order logic is quite satisfactory. This is not the case with second order logic, especially under the light

of *certainty*. The new approach — épures — should improve the the existing systems and their interpretations: in particular, fix the limitations of the the usual realistic, semantic, approach which collapsed in front of natural numbers. By introducing deontic components — the gabarits at work in the épures —, we should able to find *derealist* integers explaining — say — why the Gödel sentence is not provable.

As to certainty, the final pattern should look like:

- A solid, i.e., non-deductive, analytic, rock in which reasoning takes place as a combination of épures.
- Depending upon the choice of the right gabarits, the access to a reasonable form of deduction.

Certainty can only be *epidictic*, i.e., rely upon a covenant between rights and duties: such a pact belongs in the realm of beliefs. But the day of true believers, of axiomatic certainty is over: the idea of an épure is to make everything, including the covenant, part of the logical artifact. Making suppositions part of the object is a way to get, once for all, rid of these presuppositions which so badly hinder logic.

References

1 J.-Y. Girard. **The Blind Spot: lectures on logic**. European Mathematical Society, Zürich, 2011. 550 pp.

Institut de Mathématiques de Luminy,
UMR 6206 – **CNRS**,
163, Avenue de Luminy, Case 907,
F-13288 Marseille Cedex 09
girard@iml.univ-mrs.fr

NON SI NON LA