CWI Quarterly Volume 9 (1 & 2) 1996, pp. 25 – 30

Propositional Connectives and the Set Theory of the Continuum

Andreas Blass [1]
Mathematics Department, University of Michigan, Ann Arbor, MI 48109, U.S.A.
e-mail: ablass@umich.edu

This talk is a survey of two topics of recent interest in mathematical logic, namely linear logic and cardinal characteristics of the continuum. I shall try to explain enough about each of them to be able to point out how they are connected. Since the underlying ideas of the two topics are quite different, I regard the existence of a connection as surprising.

1. Linear Logic

What does an implication, $A \Rightarrow B$, mean? According to classical logic, $A \Rightarrow B$ is true if and only if either A is false or B is true (or both). This is regarded as specifying the meaning of implication because, quite generally, classical logic finds the meaning of a statement in the conditions for its being true.

According to constructive logic, as developed by Brouwer and Heyting, a proof of $A \Rightarrow B$ is a construction converting any proof of A into a proof of B. This is regarded as specifying the meaning of implication because, quite generally, constructive logic finds the meaning of a statement in what is required to prove it.

Two close relatives of the Brouwer-Heyting interpretation of implication are Kolmogorov's interpretation in terms of problems and the Curry-Howard interpretation in terms of types. Kolmogorov regarded statements as representing problems and interpeted $A \Rightarrow B$ as the problem of reducing B to A, i.e., of solving B given a solution of A. Curry and Howard pointed out a correspondence between logical systems and type theories, where propositions correspond to types (which can safely be regarded simply as sets for the purposes of this talk)

[1] I thank the organizers of the SMC50 Congress for inviting me to give this talk, and I thank the NSF for partial support under grant DMS-9505118.

and $A \Rightarrow B$ is the type of functions from type A to type B. If we identify a proposition with the type of its proofs (and identify constructions with functions) then the Curry-Howard correspondence amounts to the Brouwer-Heyting interpretation.

The Curry-Howard corespondence has been of interest recently in theoretical computer science, where one deals with data types and where $A \Rightarrow B$ could be the type of procedures with a formal variable of type A and a value of type B.

The preceding comments about implication have analogs for other connectives. For example, the conjunction $A \wedge B$ is defined classically as being true whenever both A and B are true. It is defined constructively by saying that to prove $A \wedge B$ one must give a proof of A and a proof of B. Under the Curry-Howard correspondence, conjunction becomes the cartesian product of types.

The first central idea of linear logic, introduced in the mid-80's by Girard, is to keep track of how often a hypothesis is used in deducing a conclusion; equivalently (via the Curry-Howard correspondence) one keeps track of how often an input is used in computing an output. This and related concepts seem (to me) more intuitive in the context of "ability to perform actions" rather than "knowledge of facts," for knowledge is (normally) permanent and re-usable while abilities can be limited in the sense that someone who can do A and can do B may not necessarily be able to do both. Although it is unclear in the context of traditional set theory what it would mean for a function to use an argument a particular number of times, the notion is considerably clearer for algorithmic procedures (and is useful for memory management).

The formal development of linear logic is based on a sequent calculus. In traditional logic, $\Gamma \vdash \Delta$, where Γ and Δ are lists of statements, means that the conjunction of the statements in Γ entails the disjunction of the statements in Δ. The first step toward linear logic is to abolish the rule of contraction,

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta,}$$

which formalized the idea that hypotheses can be re-used: One hypothesis A is as good as two copies of it. The removal of the contraction rule results in a system called affine logic. In it, a sequent $\Gamma \vdash \Delta$ carries the additional information that each hypothesis is to be used at most once.

Linear logic is obtained from affine logic by also abolishing the rule of weakening,

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta,}$$

which formalized the idea that a hypothesis can be ignored. In linear logic, $\Gamma \vdash \Delta$ requires that each hypothesis in Γ is used exactly once.

There is also a non-commutative version of linear logic, abolishing the rule of exchange,

$$\frac{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}{\Gamma_1, B, A, \Gamma_2 \vdash \Delta.}$$

Then $\Gamma \vdash \Delta$ requires that the hypotheses be used in the order listed.

Girard and others have developed linear logic quite extensively, especially its proof theory, but considerably less is known about non-commutative linear logic. From now on, I shall talk only about the commutative system.

Linear logic's insistence that hypotheses be used just once raises a question about the meaning of conjunction. Should one use of A and one use of B constitute one or two uses of $A \wedge B$? Girard's answer is that there are two sorts of conjunction, for which he introduced the notations $A \otimes B$ and $A\&B$. One use of $A \otimes B$ consists of a use of A and a use of B. One use of $A\&B$ consists of one use of A or one use of B, whichever the user wants. (Notice here the beginning of an interaction between the hypotheses and a "user.") These two conjunctions are governed by the rules of inference

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A\&B} \qquad\qquad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B}.$$

(These rules would be equivalent in the presence of contraction and weakening.)

The interaction alluded to above, between a user requesting information and hypotheses supplying information, or, in more customary terminology, between questions and answers, leads to the second central idea of linear logic, namely linear negation, the operation that interchanges questions and answers. An answer of type $A^{\perp}$ is a question of type A and vice versa.

There have been several attempts to model semantically this sort of interaction. I introduced a game semantics, where propositions (or types) are modeled by games, whose rules specify how the questioner and answerer are to interact. This semantics was modified by Abramsky, Jagadeesan, Hyland, and Ong to improve its correspondence with Girard's proof theoretic system.

I shall not discuss these developments further here but instead concentrate on a simpler semantics, a special case of de Paiva's "Dialectica-like" semantics. Here a proposition is represented by a triple $\mathbf{A} = (A_-, A_+, A)$ where A_- is the set of "questions of type $\mathbf{A}$," A_+ is the set of "answers of type $\mathbf{A}$," and $A \subseteq A_- \times A_+$ is a binary relation holding between any question and its "correct" answers.

By a morphism from $\mathbf{A}$ to $\mathbf{B}$, I mean a pair of functions $\alpha : B_- \to A_-$ and $\beta : A_+ \to B_+$ such that, for all $b \in B_-$ and $a \in A_+$,

$$\alpha(b) A a \Rightarrow b B \beta(a).$$

In the presence of such a morphism, if you can answer questions of type $\mathbf{A}$, then you can also answer questions of type $\mathbf{B}$; given a question in B_- convert it with α into a question in A_-, produce an answer in A_+, and convert it with β into an answer in B_+ for the original question.

Linear negation is modeled by interchanging questions and answers and interchanging correct and incorrect.

$$\mathbf{A}^\perp = (A_+, A_-, \neg\breve{A}).$$

The connectives $\otimes$ and $\Rightarrow$ are modeled by

$$\mathbf{A} \otimes \mathbf{B} = (A_-^{B+} \times B_-^{A+}, A_+ \times B_+, K),$$

where $(f,g)K(a,b)$ iff $f(b)Aa$ and $g(a)Bb$, and

$$\mathbf{A} \Rightarrow \mathbf{B} = (\mathbf{A} \otimes \mathbf{B}^\perp)^\perp = (A_+ \times B_-, A_-^{B-} \times B_+^{A+}, C),$$

where $(a,b)C(f,g)$ if either not $f(b)Aa$ or $bBg(a)$. (In using the notation $\Rightarrow$, I deviate from the standard notation for this linear implication. Unfortunately, the standard notation, a dash with a little circle at the right end, is not in standard TEX.) One pleasant consequence of these definitions is that a morphism $\mathbf{A} \to \mathbf{B}$ is an answer (f,g) that is correct for every question (a,b) in the sense of $\mathbf{A} \Rightarrow \mathbf{B}$. De Paiva showed that, with suitable interpretations for the remaining connectives, Girard's proof system is sound for this semantics. In addition, as we shall see in the next section, parts of this semantics arise naturally in a quite different context.

2. Cardinal Characteristics of the Continuum

One of set theory's earliest and most useful contributions to the rest of mathematics was the distinction between different infinite cardinals and especially the distinction between countable infinity ($\aleph_0$) and the cardinality of the continuum ($\mathfrak{c} = 2^{\aleph_0}$). This made it possible to do things in some infinite situations (countable ones) that would be impossible for continuum-sized ones. Examples include the Baire category theorem and the countable additivity of Lebesgue measure. Whenever, as in these examples, $\aleph_0$ and $\mathfrak{c}$ behave differently, one can ask where between these the behavior changes. Of course, if one believes the continuum hypothesis (CH), i.e., $\mathfrak{c} = \aleph_1$, then this question is trivial. But it is consistent with the usual axioms of set theory (ZFC) that there are (many) cardinals between $\aleph_0$ and $\mathfrak{c}$, and then it is reasonable to consider cardinals like the following.

- $\mathbf{cov}(\mathbf{B})$ is the minimum number of meager sets (countable unions of nowhere dense sets) whose union is $\mathbb{R}$. (The "B" stands for Baire.)
- $\mathbf{add}(\mathbf{B})$ is the minimum number of meager sets in $\mathbb{R}$ whose union is not meager.
- $\mathfrak{d}$ is the minimum number of functions $\mathbb{N} \to \mathbb{N}$ needed to eventually dominate every such function.
- $\mathfrak{b}$ is the minimum number of functions $\mathbb{N} \to \mathbb{N}$ such that no single function eventually dominates them all.

These and many other cardinal numbers of a similar nature are called cardinal characteristics of the continuum, and many connections (mostly inequalities) are known between them; there are also many independence results saying that different values of these characterisitics are consistent with ZFC.

For the cardinals defined above, the provable inequalities include

$$\aleph_1 \le \mathbf{add}(\mathbf{B}) \le \left\{ \begin{matrix} \mathfrak{b} \\ \mathbf{cov}(\mathbf{B}) \end{matrix} \right\} \le \mathfrak{d} \le \mathbf{2}^{\aleph}\mathbf{0}.$$

The characteristics for Baire category defined above have analogs for Lebesgue measure; just replace “meager” with “measure zero” in the definitions and replace “B” with “L” in the notations. It is a surprising theorem of Bartoszyński that $\mathbf{add}(\mathbf{L}) \le \mathbf{add}(\mathbf{B})$. This inequality (like each of the inequalities exhibited above) can consistently be strict and can consistently reduce to equality.

The definitions of many of the cardinal characteristics and the proofs of many of the inequalities between them (including all those mentioned above) fit into the following framework, apparently first used by Miller and Fremlin and explicitly formulated by Vojtáš.

For two sets A_- and A_+ and a relation $A \subseteq A_- \times A_+$ (as in de Paiva's semantics described in the preceding section), define

$$\|(A_-, A_+, A)\| = \min\{|Z| \mid Z \subseteq A_+ \text{and} (\forall x \in A_-)(\exists z \in Z)\, xAz\}.$$

Such “norms” include all the characteristics defined above:

Let M be the set of meager sets (or codes for meager F_σ sets). Then

$$\mathbf{cov}(\mathbf{B}) = \|(\mathbb{R}, \mathbf{M}, \in)\|,$$

$$\mathbf{add}(\mathbf{B}) = \|(\mathbf{M}, \mathbf{M}, \not\supseteq)\|.$$

Let $\le^*$ be the eventual majorization ordering on $\mathbb{N}^\mathbb{N}$. Then

$$\mathfrak{d} = \|(\mathbb{N}^\mathbb{N}, \mathbb{N}^\mathbb{N}, \le^*)\|,$$

$$\mathfrak{b} = \|(\mathbb{N}^\mathbb{N}, \mathbb{N}^\mathbb{N}, \not\ge^*)\|.$$

If there is a morphism $\mathbf{A} \to \mathbf{B}$ then $\|\mathbf{A}\| \ge \|\mathbf{B}\|$. All the inequalities mentioned above can be deduced from this general fact by constructing explicit morphisms. Since the inequalities all become trivial when CH holds, I once hoped that the existence of morphisms might remain non-trivial and capture, even in the presence of CH, the essential content of the proofs of the inequalities. Yiparaki showed that this is not the case; CH provides morphisms as well as inequalities. But it does not provide Borel morphisms (i.e., morphisms whose components α and β are Borel functions), while the usual proofs of the inequalities do produce Borel morphisms. So at the moment, Borel morphisms seem to capture the essence of the usual proofs of these inequalities.

There are a few known inequalities involving three cardinal characteristics. A nice example, due to Miller, is

$$\mathbf{add}(\mathbf{B}) \ge \min\{\mathbf{cov}(\mathbf{B}), \mathfrak{b}\}.$$

(The reverse inequality follows from those displayed earlier.) The proofs of this and similar examples can be formalized in terms of morphisms to objects constructed by means of (the dual of) the following "sequential composition" connective.

$$\mathbf{A};\mathbf{B} = (A_- \times B_-^{A_+}, A_+ \times B_+, S),$$

where $(x, f)S(a, b)$ iff xAa and $f(a)Bb$. This is closely related to de Paiva's interpretation of the $\otimes$ of linear logic, but it is not commutative. In fact, the order of sequential composition is crucial in proofs of inequalities like the one above. It essentially corresponds to the order of arguments and constructions in proofs of inequalities. In many cases, it also corresponds to the order in which forcing constructions should be iterated in order to produce models with certain special properties. In other cases recently studied by Mildenberger, forcing cannot detect the order of steps, or even the need for several steps, but subtler, combinatorial arguments can.