Electronic Notes in Theoretical Computer Science,
3, 1996. 22 pages

Intuitionism – Counting its Blessings

Dirk van Dalen

Abstract. A brief survey of the impact of intuitionistic logic and mathematics on modern practice is presented. The main influence is via the so-called "BHK interpretation" (or "proof interpretation"). By somewhat relaxing the conditions on the notion of proof the familiar notions of 'realizability', 'Curry-Howard isomorphism' etc. are motivated. Also some attention is paid to the characteristic process of replacing traditional notions by strong positive ones.

1 The paradox of success

The history of intuitionism affirms the general rule of success in science: once a topic or notion has been successfully adopted by the scientific community, its founder and origins become almost irrelevant to the user. Examples are all around us: nobody quotes Euclid when doing geometry, or Newton or Leibniz when differentiating a function. Even notions or areas called after their creators loose the association with the persons, e.g. hardly anybody thinks of Euclid when mentioning euclidean geometry, or of Turing when writing down a Turing machine. Perhaps the real mark of success is a dissociation of the notion from its creator (In modern terms: the ultimate success of a scientist consists of a gradual withdrawal from the citation index). In the case of intuitionism this kind of success has been attained. Few people will still think of Brouwer when they use bar-induction, or appeal to the continuity theorem, and even fewer will cite Brouwer. After the boom of the sixties-seventies in the foundations of mathematics, intuitionism has lost its controversial character and became accepted within the larger framework of constructivism. Its methods and insights have been so widely recognized, that it mostly seems to live on as an adjective (as in intuitionistic logic). Its success has killed the topic as an independent area of research in mathematics or logic. It has become part of a wider tradition of constructivism.

Contrary to Brouwer's expectations and hopes, intuitionism has found its acceptation by way of logic and computer science, rather than in mathematics.

As a consequence of the present position of intuitionism in the wider context this talk will deal with general issues in constructivity and not just in intuitionism. To make the distinction clear: *intuitionism is based on the mental, intellectual activity of the individual, and it derives its objects and principles* *from this source. Constructivity, on the other hand, is a philosophy free part of mathematics and logic which studies algorithmic aspects.*

2 The heritage of intuitionism

The three principal areas where Brouwer left his mark, are *objects, methods* and *principles*. The first two are closely connected, and the third one is the result of reflection on them. Brouwer's basic innovation in the domain of objects is the notion of *choice sequence*. Choice sequences (say of natural numbers) provide us with an element of uncertainty (unpredictability), which lends a new complexion to the mathematical universe. The introduction of incomplete objects (or objects with incomplete information) automatically forces another logic on the user. Let us recall one of those familiar example of intuitionistic mathematics: how does one show that if the decimal expansion of π contains 100 consecutive sixes, it also contains 99 consecutive sixes? The truth table wisdom fails here; we cannot assert that either there are no 100 consecutive decimals six in π's expansion or there are 99 consecutive decimals six in π. For, we simply are in no position to make the decision. Instead we have to adopt a more effective procedure: as soon as we have proof that there are 100 consecutive sixes in π's expansion (which means that we can pinpoint the sequence), we can provide a proof that there are 99 consecutive sixes in the expansion. So how do we get the conviction that the proof of the first statement leads to the proof of the second statement? The answer is: we have an algorithm that converts proof 1 into proof 2. This is the basic of idea of the proof interpretation: ; so one has to adopt the proof-interpretation (or some variation): a proof of $A \to B$ is an algorithm that converts a proof of A into a proof of B. Such an algorithm has to be a finite object, after all we want to convince, if not others, at least ourselves. So intuitionism has brought us the double feature of finitary objects (natural numbers, rationals, operations, proofs) and infinitary objects (choice sequences, sets), complete with its own logic and intended semantics. It is important to note that Brouwer introduced a novelty in mathematics that might easily have escaped the attention of the contemporaries, had not Heyting and Kolmogorov presented the matter in a systematic approach. For Brouwer, proofs were constructions of a particular kind, and so they were part and parcel of mathematics itself, not a phenomenon in another medium (i.e. language). Proofs were actual objects to be constructed and to be operated upon.

3 The influence on modern practice

Apart from its philosophical impact, intuitionism has influenced mathematics and computer science along two-initially separate lines: the algorithmic and the semantic lines. The algorithmic line starts with Kleene in 1945; the semantic line is much older, it dates back to the middle thirties.

Both the semantical and the algorithmic tradition have their strong and weak points. The algorithmic tradition has some strong claims to superiority, in face of the basic claim of constructive and intuitionistic mathematics: it provides programmable algorithms instead of intuitive constructivity.

Girard, [G 95], has quite correctly pointed out that mathematicians tend to consider the subject matter of mathematics as rigid and eternal, whereas computer science has introduced dynamics and structures with states. Whereas this is undoubtedly the case for classical mathematics, which is frozen from the outset by its adherence to the principle of the excluded middle, intuitionistic mathematics is far more modest in its eternity claims. The explicit insistence on potential infinity, together with the adoption of incomplete (in time!) objects, lends intuitionism a dynamic feature, for which it does not have to introduce an explicit time parameter, as in classical mathematics. This may serve as a partial explanation of the modest popularity of intuitionistic methods in computer science.

4 Theme and Variations: Existence yields algorithms

The theme of the intuitionistic logic is the proof interpretation, and the variations were composed by Kleene, Kreisel, Gödel, Curry-Howard, Martin-Löf and others. The significance of the theme and its variation can hardly be overrated. Building on the idea of the proof interpretation a number of "models" have been introduced that each take advantage of certain aspects of constructive mathematics. In exchange for the efforts invested in the codification of variation of proof-notions, one would like to ash in on effectiveness. To be precise, the mark of success here is the "existence property" or the "effective definability property": if $\exists x Ax$ is proved constructively, there should be an effective procedure to compute (or define) an object a and a proof of Aa. In addition to Martin-Löf's type theory the typed lambda-calculus should be mentioned as a manifestation of the proof-interpretation. The success of type theories of various orders is highly gratifying from an intuitionistic point of view. It shows that the fundamental ideas underlying the constructive truth notion are sufficiently robust to be realised under a large range of conditions.

In the sixties Kreisel listed a number of requirements for the proof interpretation, [Kr 65]; the most important of which was the decidability of the proof relations: "one recognizes whether p is a proof of A". This decidability is conceptually plausible, and in a number of instances – e.g. the standard proof-predicate, or the natural deduction derivation – it is satisfied. However, for the fruitfulness of the idea of the proof-interpretation it is often necessary to be somewhat liberal, and to drop one or more basic restrictions. It is by now generally accepted that the proof interpretation (or the problem interpretation of Kolmogorov; the names of the Heyting and Kolmogorov are lumped together with the name of the founding father in the term "BHK-interpretation") underlies most of the constructive interpretations of logic. It is a general methodological fact that the fruitfulness of a paradigm is increased by avoiding undesirable precision; this applies well in the case of the proof interpretation – one has to allow for a measure of freedom in selecting the criteria.

The proof-interpretation has turned out to be a powerful heuristic tool. A warning is in order here: even the truth table interpretation can be viewed as a degenerate proof interpretation, with just one proof object. So the general applicability also carries its weakness.

If we, for the moment describe the business of constructive mathematics and its logic as the analysis of the algorithmic content of mathematics, then it is obvious that we should look for algorithmic interpretations of one sort or another. We will look at a number of those and trace their development.

4.1 Kleene's 1945 Realizability

Kleene viewed the interpretation of quantifiers (say over natural numbers) along the line of the finitary standpoint of Hilbert-Bernays.[1] Quantified statements are viewed as incomplete statements, or statements with incomplete information. The meaning of $\exists x A(x)$ thus has to be completed by an instance n such that $A(n)$. Combining the intuitionistic proof interpretation with the "incomplete" information notion, Kleene implemented the basic notions in terms of partial recursive functions [K 45]. He boldly extended the 'incomplete information' idea to *all* connectives.

We will show the main points of the proof interpretation and realizability in the table below. The notation is:

proof interpretation	a is a proof of A	–	$a : A$
realizability	a realizes A	–	$a\ \mathbf{r}\ A$)

In the proof interpretation "a is a proof of A" is primitive, i.e. it stands for the unformalized proof notion. In realizability natural numbers realize statements.

[1]Who seem to be indebted, in turn, to Hermann Weyl, cf. [**?**].

In our notation we freely use the apparatus of recursion theory, e.g. $\{a\}b$ for application, $(a)_i$ for projection, etc.

A	$a : A$	$a \mathbf{r} A$
$A_1 \wedge A_2$	$a = \langle a_1, a_2 \rangle$ and $a_1 : A_1,\ a_2 : A_2$	$(a)_0 \mathbf{r} A_1$ and $(a)_1\ r\ A_2$
$A_1 \vee A_2$	$a = \langle a_1, a_2 \rangle$ and $(a_1 = 0$ and $a_2 : A_1)$ or $(a_1 \neq 0$ and $a_2 : A_2)$	$((a)_0 = 0 \wedge a_2 \mathbf{r} A_1) \vee$ $((a)_0 \neq 0 \wedge a_2 \mathbf{r} A_2)$
$A_1 \rightarrow A_2$	a is a construction such that if $b : A_1$, then $a(b) : A_2$	$b \mathbf{r} A_1 \rightarrow \{a\}b\ \mathbf{r} A_2$
$\forall x A(x)$	a is a construction such that $a(n) : A(n)$ for all n	$\{a\}n \mathbf{r} A(n)$ for all n
$\exists x A(x)$	$a = \langle a_1, a_2 \rangle$ and $a_2 : A(a_1)$	$(a)_1 \mathbf{r} A((a)_0)$

The realizability clauses are faithfully mimicking those of the proof interpretation, and so realizability can be viewed as a particular, constructive truth definition. It should not surprise us that by narrowing down the meaning of "a is a proof of A", we obtain a theory which is actually richer than the originally intended theory, i.e. **HA** in this case. It came, however, as a surprise that the theory of realizable arithmetic can indeed be a few meaningful statements,[2] the key role here is played by:

Church's Extended Thesis:

$ECT_0 \qquad \forall x(A(x) \rightarrow \exists y B(x,y) \rightarrow \exists z \forall z(A(x) \rightarrow B(x, \{z\}x))$
for $\exists$-free A.

Fact:

- $\mathbf{HA}^* + ECT_0 \vdash A \leftrightarrow \exists x(x \mathbf{r} A)$ and
- $\mathbf{HA}^* + ECT_0 \vdash A \Leftrightarrow \mathbf{HA} \vdash \overline{n}\mathbf{r} A$ for a numeral $\overline{n}$,

where $\mathbf{HA}^*$ is a suitable extension of **HA** in which partial terms are allowed, and which allow for a formalization of the basics of recursion theory, cf. [TD 88].

Kleene's realizability was the first of a long sequence of realizability notions, which are more or less variations on the original notion.

One of such notions is the "truth-realizability", which is obtained from Kleene's realizability by an extra condition in the implication clause:

[2]the material on realizability, modified realizability and the Dialectica interpretation is mostly drawn from [T 73] and [T 92]

x **rt** $(A \to B) := \forall y(y$ **rt** $A \to \{x\}(y)$ **rt** $B) \wedge (A \to B)$

One of the attractive aspects of realizability is that it makes the relation between existential statements and instantiations explicit. The truth realizability is in particular useful in this respect. One shows that:

$\mathbf{HA}^* \vdash t$ **rt** $A \to A$ and

$\mathbf{HA}^* \vdash A \Rightarrow \mathbf{HA}^* \vdash t$ **rt** A for a suitable term t.

One may use this fact to get an effective version of the numerical existence property

$\mathbf{HA}^* \vdash \exists x A x \Rightarrow \mathbf{HA}^* \vdash A\overline{n}$ for a suitable $\overline{n}$.

In fact, **HA** is closed under Church's Rule:
$\mathbf{HA} \vdash \forall x \exists y A(x, y) \to \mathbf{HA} \vdash \forall x A(x, \{e\}y)$ for a suitable e.

Since the index of the recursive (choice) function can be effectively determined, realizability provides a (not albeit extremely realistic) program extradition machinery. The idea is, however, basic for some more realistic versions, which we will discuss later.

5 Kreisel's modified realizability

.

More than a decade after Kleene's pioneering papers, an essentially different realizability notion was introduced by Kreisel; this version is now known as *modified realizability*. Whereas Kleene's realizability is basically a first-order technique, modified realizability is a technique for typed systems. The present versions are formulated for $\mathbf{HA}^\omega$, the higher-type extension of Heyting's arithmetic. $\mathbf{HA}^\omega$ is a type theory with product and function types, its formalisation is well-known, following the formulation of Gödel's system **T**. Apart from the usual axioms for the traditional combinators, it has a recursor at all types and an accompanying recursion axiom.

The clauses for modified realizability run as follows: (the types of the terms are not indicated, but they don't present problems).

x **mr** $(t = s) := t = s$ (for numerical terms)

$x \ \mathbf{mr} \ (A \wedge B) := p_0 x \ \mathbf{mr} \ A \wedge p_1 x \ \mathbf{mr} \ B$

$x \ \mathbf{mr} \ (A \to B) := \forall y (y \ \mathbf{mr} \ A \to xy \ \mathbf{mr} \ B)$

$x \ \mathbf{mr} \ \forall z A(z) := \forall z (xz \ \mathbf{mr} \ A(z))$

$x \ \mathbf{mr} \ \exists x A(x) := p_1 x \ \mathbf{mr} \ A(p_0 x).$

The disjunction is not treated separately, as it is definable from $\exists$. This realizability looks rather like a translation, but one can obtain more semantical versions by interpreting $\mathbf{HA}^\omega$ itself in models, e.g. HRO.

Modified realizability, like its predecessor, allows an axiomatization in simple terms:

$\mathbf{HA}^\omega + AC + IP_{\exists f} \vdash A \Leftrightarrow \mathbf{HA}^\omega \vdash t \ \mathbf{mr} \ A$ for some t.

Here AC is the full typed axiom of choice and $IP_{\exists f}$ is the *independence of premise principle* for $\exists$-free formulas:

$(A \to \exists x^\sigma B) \to \exists x^\sigma (A \to B)$ with A $\exists$-free.

It is not hard to see that $\mathbf{HA} + M_{PR} + CT_0 + IP$ is inconsistent, where M_{PR} is the primitive recursive version of Markov's principle and CT_0 the arithmetic version of Church's Thesis. IP is the negative independence of premise principle. Since CT_0 is likewise modified realizable, it is clear that Markov's principle is not **mr** realizable. So there is a version of "recursive" arithmetic (of higher types) which violates Markov's principle.

There are numerous variations on realizability, each of them having its own specific proof theoretic features. We mention the realizability notion of Lifschitz, introduced for the purpose of proving CT_0 independent of CT_0!

In the past decades a large number of facts about formal systems of intuitionistic arithmetic has been established by means of one realizability or another.

The following is a modest selection (the reader should consult [T 73] and [T 92] for a survey of realizability):

(i) $\mathbf{HA}^* + ECT_0$ is conssistent over $\mathbf{HA}^*$

(ii) $\mathbf{HA} + ECT_0 + M \vdash A \Leftrightarrow \mathbf{HA} + M \vdash \exists x (x \ \mathbf{r} \ A)$

(iii) $\mathbf{HA} + M + ECT_0 \vdash \neg\neg A \Leftrightarrow \mathbf{PA} \vdash \exists x (x \ \mathbf{r} \ A)$

(iv) $\mathbf{HA} + IP + CT_0$ is consistent over $\mathbf{HA}$

(v) $\mathbf{HA}^\omega + IP^\omega + AC + CT_0$ is consistent over $\mathbf{HA}^\omega$

(vi) $\mathbf{HA} + CT_0 \nvdash ECT_0$ (Beeson)

(vii) $\mathbf{HA} + CT_0! \nvdash CT_0$ (Lifshitz)

(viii) $\mathbf{EL} + WCT \nvdash CT$ (where $\mathbf{EL}$ is elementary analysis)

6 Gödel's Dialectica Interpretation

.

There is one more influential implementation of the proof interpretation; the interpretation of typed arithmetic in itself via Gödel's interpretation. The similarity is not so obvious here, but for the key cases ($\rightarrow$, and $\forall$) there is an observable relationship. Consider $\mathbf{HA}^\omega$ and define for each formula A a translation A^D:

$A^D := A$ for atomic A

Now let $A^D = \exists x \forall y A_D(x, y), B^D = \exists u \forall v B_D(u, r)$, then

$(A \wedge B)^D := \exists xu \forall yv(A_D \wedge B_D)$

$(A \vee B)^D := \exists z^0 xu \forall yv(z = 0 \rightarrow A_D) \wedge (z \neq 0 \rightarrow B_D))$

$(\exists z A)^D := \exists zx \forall y A_D$

$(\forall z A)^D := \exists x \forall zy A_D(xz, y, z)$

The constructive feature of the Dialectica interpretation is of a different nature, compared to the preceding interpretations. It is rather closer to the finitistic meaning considerations of Hilbert-Bernays, or even the intuitionistic meaning consideration of Hermann Weyl. This can be seen by looking at a simple case.

Consider, e.g., $\exists x Ax \rightarrow \exists u Bu$ for atomic A and B; it is translated as $\exists U \forall x(Ax \rightarrow BUx)$. This is exactly what the finitistic interpretation yields.

There is no immediate "proof interpretation" feature here. But since explicit functionals can be found for the existential variables, and the matrix of the formula is quantifier free, a certain analogy with the constructive interpretation can be claimed.

The Dialectica interpretation can also be axiomatized; the following holds:

$\mathbf{HA}^\omega + IP_0' + M' + AC \vdash A \leftrightarrow A^D$,

where $IP_0' = (\forall x A x \to \exists y B y) \to \exists y(\forall x A x \to B y)$ and
$M' = \neg\neg\exists x A x \to \exists x A x$ for quantifier free A, with arbitrary x.

7 Effectivity and Feasibility

.

¿From a constructive viewpoint the above implementation of the "proof-interpretation" idea is very gratifying, in as far as it carries the idea beyond that of a mere heuristic instrument. It has a serious drawback, however. The resulting algorithms are highly complex and the machinery involved does not seem to suggest immediate relations between the formula to be interpreted and the resulting algorithm (say for $\exists x A x$ and its instantiating algorithm).

A desideratum, here, is a method that allows control over the complexity of realizing objects.

Some attempts have been made in this direction. There is a recent paper of Damnjanovic [D 95], dealing with the problem for Kleene-realizability.

Damnjanovic showed that one may essentially restrict the class of (indices of) realizing functions. In fact the so-called ϵ_0 -recursive functions are sufficient to obtain a sound realization of **HA**. Moreover, his method shows that the realizability is minimal in a specific sense: a rise in complexity corresponds to the use of sensitive rules of the formal system, e.g. $\to$-elimination, $\forall$-elimination, induction. Thus he incidentally recovers a result of Kreisel which says that the definable functions of **HA** are the ϵ_0-recursive ones, as a special case of the following:

If $\mathbf{HA} \vdash \forall x \exists y A(x, y)$ then for all n $A(n, f(n))$ for some ϵ_0-recursive function (there is also a version for arbitrary types).

Cook and Urquhart had also approached the problem of improving on realizability and on the Dialectica interpretation in their '*Feasible interpretation of feasibly constructive arithmetic*" [CU 93]. They considered an intuitionistic first-order extension of Cook's polynomial equation calculus, and a higher-type system of feasible functionals. The authors work in a formal system **IPV** which is a predicate logic extension (with a weak form of induction) of Cook's equation calculus **PV** (*polynomially verifiable*). The system **IPV** in fact is a conservative extension of Buss' $\mathbf{IS^1_2}$. **IPV** itself is extended conservatively to a higher-type system $\mathbf{IPV}^\omega$ of typed lambda-calculus with feasible functionals, which is conservative over **IPV**. A suitable modification of the modified realizability yields results for the polynomial versions of arithmetic and functionals comparable to the older results for **HA**; for the existence property holds:

For example $\mathbf{IPV}^\omega \vdash \forall x \exists Y A(x,y) \rightarrow \mathbf{IPV}^\omega \vdash \forall x A(X, S(x))$ for a suitable closed term S of $\mathbf{IPV}^\omega$
and
$\mathbf{IPV}^\omega \vdash A(x) \vee \neg A(x) \Rightarrow \mathbf{IPV}^\omega \vdash f(x) = 0 \leftrightarrow A(x)$ for a function f in PV (i.e. predicates which are decidable in $\mathbf{IPV}^\omega$ are polynomial time computable).

There are thus indications that large parts of the realizability techniques can be fruitfully modified to a more feasible approach.

Beltiukov [Be 95] has also investigated realizability in weaker computation classes by means of a weak system of arithmetic (with concatenation), he obtains polynomial time programs, and similar results for other complexity classes (the Kalmar elementary class, the Grzegorczyk class E^2, LinSpacePolyTime).

No reflection on the role of the BHK interpretation can be considered complete without mentioning Martin-Löf's type theory. In this type theory the parallel "proofs : propositions = elements : types" has been carried to perfectness. The term-calculus for proofs and for derivations has been incorporated in an efficient generalization of Gentzen's Natural Deduction system. One of the features that distinguishes Martin-Löf's approach from earlier formulations, is its precise treatment of hypotheses, or context − by now a generally accepted practice. The major foundational importance of Martin-Löf's type theory derives, however, from stressing the importance of introduction-elimination rules for connectives and operations. Taking the hint from Wittgenstein, the importance of introduction- and elimination rules for rendering the meaning of connectives manifest in usage, has been pointed out by Dummett, Prawitz and Martin-Löf. (cf [Du 75], [Du 78], [Pr 77], [**?**], [Su 86].

Far from being content with a type-theoretical formulation of just the counterpart of predicate logic, Martin-Löf has added rules for basic mathematical notions and operations, e.g. natural numbers, well-order, universes. The type-theoretic approach is highly gratifying for a number of reasons. It provides practical, omputational procedures, but it also embodies in a systematical way various ideas and methods that have been part of the intuitionistic/constructivistic folklore.

8 Incorporating classical systems

.

Almost all of the above can be seen in the light of the extraction of information from constructive proofs. For some time, however, there have been efforts to extract – if possible - - effective information from classical proofs. Instead of trying to give a survey of these developments, we will just mention a particular topic.

The theory to be analysed is a higher-order version of Peano's arithmetic, $\mathbf{PA}^\omega$, plus the axiom of choice. To this theory Kolmogorov's double negation translation K is applied. For $\mathbf{PA}^\omega$ one gets $\mathbf{PA}^\omega \vdash A \Rightarrow \mathbf{HA}^\omega_- \vdash K(A)$, where $\mathbf{HA}^\omega$ is a minimal higher-order arithmetic (i.e. without the Ex Falso rule). In view of the classical strength of the axiom of choice, one cannot expect a corresponding result for $\mathbf{PA}^\omega \vdash AC$. The theory $\mathbf{HA}^\omega_- + K(AC)$ has to be analysed separately.

The translation $K(AC)$ is actually strong enough to allow an interpretation of the impredicative comprehension principle, hence it cannot be inferred from the intuitionistic choice axiom. Moreover, it is not neutral since it refutes Church's Thesis:

In $\mathbf{PA}^\omega$ we get $\exists f \forall x(A(x) \leftrightarrow f(x) = 0)$ for any A, and hence one can prove in $\mathbf{HA}^\omega_- + K(AC)$

$$\neg\neg\exists f \forall x[\neg\neg(f(x) = 0) \leftrightarrow \forall z \neg T(xxz)]$$

By the routine properties of recursive realizability we see that it cannot be realized, in view of the unsolvability of the Halting Problem.

By means of a suitable extension of modified realizability (formulated in a handy programming language), which contains extra realizers for $\perp$, it is shown that the theorems of $\mathbf{HA}^\omega_- + K(AC)$ are realized by closed terms not containing any of the extra constants.
Among the fall out of this modified realization there are the consistency of classical analysis ($\mathbf{PA}^\omega + AC$); a computation for the numerical existence property in $\mathbf{PA}^\omega + AC$, (that is, for formulas decidable in $\mathbf{HA}^\omega$); an effective algorithm for the $\forall x^\tau \exists y^N$ case (i.e. in the above mentioned programming language).

There is also work by Berger and Schwichtenberg on program extraction form classical proofs, e.g. the program for the gcd as a linear combination of both parts, cf. [BS 95], [BS 95*].

Finally it should be noted that there are a number of semantic proofs of the existence property for certain systems (such as $\mathbf{HA}$). As a rule these methods do not yield effective solutions, or at best, they require a certain amount of metamathematical processing before effectivity can be obtained.

9 Semantical Approaches

.

Whereas the preceding sections dealt with various theories incorporating certain aspects of constructivity, the true constructivist wishes to see a coherent account of the mathematical universe. The first such account that comes to mind is a constructive version of set theory, such as, for example, embodied in **IZF** of Harvey Friedman, or Aczel's **CZF**. However, these accounts are still on the proof theoretical side of constructive mathematics.

The semantical approach which we want to pursue here, has its roots in the thirties, when Kuratowski and Tarski introduced their topological interpretation of propositional logic. Model theory of intuitionism went through a long incubation period before it started to investigate realistic mathematical structures. After a period of more or less abstract study, as presented for example, in the comprehensive "The Mathematics of Metamathematics" of Rasiowa and Sikorski [RS 63]; the semantics of Beth, [B 56], and Kripke, [K 62], provided tools for the analysis of concrete systems, in particular arithmetic and analysis; cf [DG 71], [Sm 73], [G 81]. After Scott showed how to model real analysis in the framework of topological interpretations [S 68], [S 70], the basic theories of analysis were modelled in topological- and Beth models [Mos 73], [D 74], [D 78].

Almost simultaneously, through the efforts of Lawvere, Scott and others, category theory was discovered as basic ingredient in the semantical study of intuitionistic logic, cf. [MM 92]. In particular *topos theory* provided a unified view of the existing semantics of intuitionistic mathematics. A topos can be viewed as a particular embodiment of the (or 'a') intuitionistic set theoretic universe.

Roughly speaking a topos is a category with finite limits and colimits, which is cartesian closed (i.e. has exponents, say 'function spaces') and has a subobject classifier. The latter allows the treatment of 'subsets' and 'powersets' in the same manner as traditional set theory. In particular an intuitionistic substitute of "characteristic function" is part of the machinery.

The unifying power of categorical logic has proved to be surprising. Let us restrict ourselves for a moment to the topos-part of category theory.

Topos theory managed to give natural models of traditional intuitionistic mathematics (e.g. sheaves over a suitable topological space, such as Baire space), strongly anti-classical theories, such as the theory of lawless sequences (sheaves over Grothendieck topologies, [HM 84]), and even algorithmic universes with Church's Thesis (the effective topos, the modified realizability topos). The latter provided the link between intuitionism and Russian constructivism à la Markov, [M 71].

The semantic tradition used to be appreciated because it yielded simple consistency proofs of intuitionistic systems (mostly arithmetic, analysis or set theory); the various models allowed the non-constructive mathematician to give a meaning to the logical and mathematical notions of the intuitionist. For some time, however, models have been studied that interpret intuitionistic theories, and at the same time are part of intuitionistic mathematics. To put it in traditional language, the metamathematics of these models is intuitionistic. This opens the way to the application of model theoretic techniques on a intuitionistic scale.

We mention some examples here:

Moerdijk has constructed a non-standard model of **HA** by intuitionistic means, [M 95]. Moerdijk's model is an object in a suitable Grothendieck topos of sheaves. The model can be viewed as an elementary extension of the standard natural number object. The analogy with traditional non-standard models is fairly precise, one indeed gets results corresponding the traditional ones. E.g. for this model 'overspill' holds.

Another approach to non-standard models was given by Palmgren, [Pa 95]. He introduced certain conservative extensions of **HA**, that have a number of desired properties of non-standard extensions. In particular he applies his techniques to the testcase of the basic facts of calculus.

One can also develop the older semantics of Beth and Kripke for the interpretation of intuitionistic analysis. In [D 86] this technique is used to obtain intuitionistically correct proofs of the disjunction and existence properties for intuitionistic analysis. The trick is to apply a suitable gluing technique. Similar techniques were also applied by Moerdijk in categorical semantics, cf. [M 82]. This is by no means an exhaustive list of intuitionistically correct semantic techniques. E.g. Lipton has considered hybrids of realizability and Kripke semantics[L 95].

The topos has the pleasing feature that it generalizes (almost) all semantics that have been around, e.g. Kripke semantics, Beth semantics, the topological interpretation. In addition, it has been allowed us to conceive the realizability interpretation as semantical constructs. If we consider Kleene's realizability, then we can use the realizing numbers to obtain a truth value object. In this case it is simply the powerset of $\mathbb{N}$ (which obviously is a Heyting algebra). The 'logical operations' on $\mathcal{P}(\mathbb{N})$ are given by the realizability clauses.

Let the predicates A and B on a set X be given as mappings from X to $\mathcal{P}(\mathbb{N})$, then
$(A \wedge B)(x) = \{\langle n_1, n_2 \rangle | n_1 \in A(x), n_2 \in B(x)\}$

$(A \vee B)(x), \{\langle 0, n \rangle | n \in A(x)\} \cup \{\langle 1, n \rangle | n \in B(x)\}$

$(A \to B)(x) = \{n | \{n\}m \in B(x) \text{ for all } m \in A(x)\}$

$\perp (x) = \emptyset$

And for $A : X \times Y \to \mathcal{P}(\mathbb{N})$ put

$$\forall y A = \bigcap_{y \in Y} A(x, y)$$
$$\exists y A = \bigcup_{y \in Y} A(x, y)$$

Starting from a suitable valuation of the atoms, a valuation $[\![A]\!]$ is obtained for arithmetic statements.
On the natural numbers (as a natural number object) one defines $[\![n = m]\!] = \{n\} \cap \{m\}$.

¿From this point on, one just mimics Kleene's realizability in order to compute the truth values of the arithmetical statements. The higher-order part of the interpretation presents no problems. On the basis of the sketched interpretation one obtains a topos, called the *effective topos*, introduced by Hyland in [Hy 82]

The effective topos yields a universe in which Church's Thesis and Markov's principle hold, one which therefore can hardly be called 'intuitionistic' – 'Markovian' would be a more proper name, or perhaps 'Kleenean'.

The effective topos thus makes it clear that the phenomena which we know from first-order practice, fit perfectly well in a natural universe, where the higher-order aspects are taken of.

One particular use of the effective topos was discovered by Hyland, he constructed in *Eff* a small complete object (i.e. one having all limits). Such an object is exactly what we need in order to make a model of polymorphic typed lambda calculus. Pitts subsequently presented a logical argument to show directly that in a suitable intuitionistic universe the polymorphic lambda calculus can be modelled, [Pi 90].

The construction of the effective topos has been modified to obtain toposes for other realizabilities, e.g. modified realizability (Grayson).

Van Oosten in [O 94] extended the existing axiomatizations of first-order realizability for **HA**, and extensions, to the higher-order theory. The key-role is played, as before, by ECT, but now one also needs uniformity principles and certain parametrization axioms. The second-order one is called *Shanin's Principle*:

$$\forall X \in \mathcal{P}(\mathbb{N}) \exists A \in \mathcal{P}_{\neg\neg}(\mathbb{N}) \forall n \in \mathbb{N}[n \in X \leftrightarrow \exists y \langle y, n \rangle \in A].$$

It should be noted that independent of the topos development of realizability, D. McCarty has carried out a cumulative model construction for $IZF+CT$, based on Kleene's realizability. He has observed a number of metamathematical features of life in a universe with Church's Thesis, [M 91].

E.g. there is quite a number of examples of the two extremes of 'lean' and 'fat' sets. Among the first there are ω-*enumerable* sets (called *sub-countable* by McCarty); there is a large supply of those, e.g. all sets with a stable equality (hence all sets with an apartness relation). Among the fat ones we find the so-called *uniform* sets, i.e. those satisfying the uniformity property:

$$\forall x \in X \forall n \in \mathbb{N} A(x,n) \to \exists n \forall x \in X A(x,n).$$

There are lots of sets satisfyinf the uniformity principle, in particular all power sets do.

Furthermore he observed that, assuming Church's Thesis, one can show that **HA** has no non-standard models. [M 91].

10 The type theories

.

It was observed long ago by Curry that there is a striking similarity between types and propositions [CF 58]; schematically given by:

$$\frac{proof}{proposition} = \frac{element}{type}$$

Howard extended Curry's ideas to the full language, he coined the phrase "Formulae-as-Types". Howard's ideas circulated in the sixties, but were only published in 1980 [Ho 80].

The type theoretic approach is almost a literal copy of the proof interpretation, indeed, one can write down just one table for the operators and interpret them in two ways.

proof : proposition		element : type
$\langle a_1, a_2\rangle : A \wedge B$	$a_1 : A$ and $a_2 : B$	$\langle a_1, a_2\rangle : A \times B$
$\langle a_1, a_2\rangle : A \vee B$	$a_1 = 0$ and $a_2 : A$ or $a_1 \neq 0$ and $a_2 : B$	$\langle a_1, a_2\rangle : A + B$
$c : A \to B$	for all $a \quad a : A \Rightarrow c(a) : B$	$c : B^A$
$c : \forall x{:}P.A(x)$	for all $p \quad p : P \Rightarrow c(p) : A(p)$	$c : \Pi x{:}P.A(x)$
$\langle a_1, a_2\rangle : \exists x{:}P.A(x)$	$a_1 : P$ and $a_2 : A(a_1)$	$\langle a_1, a_2\rangle : \Sigma x{:}P.A(x)$

This formulation suggests a term calculus for proofs or elements, analogous to typed lambda-calculus as the companion for the implicational fragment.

One can them ‘update’, so to speak, Gentzen’s natural deduction system with proof terms; cf [TD 88], 556, [Gal 95], [GLT 89].

This idea has further led to a systematization of the natural extensions of simple typed lambda-calculus, as laid down in Barendregt’s cube, [Ba 92]. All this illustrates the striking fruitfulness of the proof interpretation.

The proof interpretation and linear logic.

Although the heuristic and even technical value of the proof interpretation may be generally accepted, there still is the challenge of fitting the new basic ideas of linear logic into the intuitionistic framework. In other words, how do we make sense of the key notions of linear logic : parallelism and resource bounds. The technical issue how to find a suitable underlying term calculus to accompany linear logic has been addressed and has the same significance as in ordinary logic. The problem is to see if the traditional explanation has anu relevance to linear logic

It may, of course, be the case that mathematics and linear logic are and will be fundamentally separated areas (cf [G 95]), but that seems a defeatist viewpoint. After all, even if mathematics tends to foster time and resource independent methods and results, there could very well be foundational questions related to these issues.

Let us return to the roots of Brouwer’s mathematics. The basic phenomenon is ‘move of time’, from this the whole of mathematics follows more or less automatically. This seems drastically at odds with paralellism, for how could the subject experience two causal sequences simultaneously? This is partly because we view time as externally given, but in fact, time is the result of the activity of the subject, i.e. the subject classifies one sensation as ‘after’ another sensation.

Hence time is somewhat loosely introduced, the decisive point is not what processes go in the subjects mind, but on which one he concentrates. So parallelism is by no means excluded, it is only that the subject can pay attention to one phenomenon at the time. ¿From a pragmatic point of view parallelism is even preferable to sequentialism, since it does away with the need of coding, or similar techniques, such as interleaving, to handle more than one choice sequence at the time. The sort of parallelism involved in linear logic, e.g. in & and $\oplus$ can be handled in a constructive basis theory just as Girard explains them, the distinction being indeed that of the subject may consciously make a choice between two events through an act of will, whereas he could also remain inert and wait for the next (sensation of an) event.

The issue of resource boundedness seems more problematic, for not only in classical, but also in intuitionistic logic "once true - always true" holds.

On Brouwer's view, the individual has in practice an imperfect memory, but for the purpose of a systematic treatment of mathematics (and science in general) he stipulated an unbounded perfect memory. He indeed, at certain places, left open the possibility that the individual had to prove the same fact over and over again. So there is no a priori why one should not take a bound on the memory capacity into account. This means that one is not automatically justified in reusing assumptions. Unfortunately this kind of consideration seems not good enough to take the drastic actions that linear logic requires. Even worse, it is hard to see how one can develop a systematic logic on the basis of possible limitations of the subjects. For the moment it seems best to accept the justifications of traditional logic and linear logic as distinct idealizations of forms of argumentation.

11 In Praise of positive notions

.

Finally a few words on a particular aspect of the actual practice of constructive mathematics.

In realistic theories of mathematics there are certain notions that cannot be dispensed with. The prime example is identity! Identity is inextricably tied up with the structures one is dealing with. A comparable place is taken by its negation, 'inequality'. In constructive theories one is often served better by positive versions of negative notions.

A familiar example is the apartness relation which strengthens the inequality relation:

$$a \# b \to a \neq b, \text{ but in general } a \neq b \not\to a \# b.$$

An explanation of this fact is that apartness on the reals is existential by nature, whereas inequality is a negative notion:

$$a\#b \text{ if there is a } 2^{-k}\text{-neighbourhood of } a \text{ separating it from } b.$$

This makes it prima facie stronger than the usual 'inequality'. Apartness was axiomatized by Heyting in the following elegant form:[H 27],

$$\begin{array}{l} a\#b \to b\#a \\ a = b \leftrightarrow \neg a\#b \\ a\#b \to a\#c \vee c\#b \end{array}$$

Observe that this immediately yields the stability of $=$: $\neg\neg a = b \leftrightarrow a = b$.

Appartness is not just the invention of intuitionists for foundational reasons, for many purposes it cannot be dispensed with, e.g. in fields $a\#0$ is equivalent to invertibility of a.

The idea of replacing negative notions by positive ones is fruitful in situations beyond that of simple identity. In constructive algebra one needs some positive notion to supplement the familiar notions of normal subgroup, ideal, etc. The positive counterparts of these notions are indicated by the prefix 'anti'.

E.g. an *anti-ideal* in a ring with an apartness relation is a subset A satisfying

$$\begin{array}{l} 0 \notin A \\ x + y \in A \to x \in A \vee y \in A \\ xy \in A \to x \in A \wedge y \in A \end{array}$$

It appears that anti-ideals are the natural things to carry out the standard constructions, such as that of quotient ring. To be precise, quotient of a ring over the complement of an inhabited anti-ideal (which is a proper ideal) has a natural apartness relation. This feature was already observed by Heyting in 1941, in the content of polynomial rings [H 41], cf [TD 88], Ch.8.

The adaptation of algebra to structures with apartness turns out to be non-trivial. E.g. the construction of free groups with apartness asks for rather strong properties of the apartness relation on the generating set, cf. [DV 88].

Recently Von Plato, [Pl 95], has picked up the thread of geometry with apartness. He similarly advocates the use of positive notions on the grounds that equality requires infinite precision, which is alien to constructive mathematics. Apartness on the other hand, only requires rough estimates. Plato's geometry project combines two natural constructive features: a constructive approach to the subject, combined with a incorporation in a suitable type system, so that one may apply the available techniques of proof checkers.

Geometry provides another (albeit first-order) example of the success of positive substitutes. In geometry one can go one step beyond apartness with one sort, and consider, e.g. 'outside' as a positive relation between points and lines, or points and planes. This too, was observed by Heyting in [H 27]; for the role of 'outside' see further [D 96].

Needless to say that the apartness relation plays an important role in topology. The very least one wants, is to have one's topology compatible with apartness:

$\{a|a\#b\}$ is open
$a \in U \to b \in U \vee a\#b$ for any open U and points a, b

Spaces satisfying these conditions are called *separated*. For most mathematical applications it is obvious that separation is required.
It is a experimental fact that one cannot restrict mathematics to structures with decidable equality, if only because the introduction of quotient structures are bound to have non-decidable equality. For that reason, it seems a sound methodology to introduce positive notions at an early stage, so that as much constructive information as possible can be handled. For computer science this seems less urgent, as it mostly deals with data structures with decidable equality. On the other hand the infinitary objects of computer science may eventually call for techniques as outlined above.

In conclusion we may say that intuitionism has enriched mathematics and logic with a number of notions and principles which in one way or another embody the basic features of constructivesness. It does not downright provide algoritms or bounds, but it rather points at the mechanisms that are implicit in the idea of effectivity.

References

[AGM 92] Abramsky, S. , D.M. Gabbay, T.S.E. Maibaum (1992) *Handbook of Logic in Computer Science, 2.* OUP. Oxford.

[Ba 92] Barendregt, H.P. (1992) Lambda Calculi with Types. In [AGM 92], 117-309.

[B 85] Beeson, M. (1985) *Foundations of Constructive Analysis.* Springer Verlag, Berlin.

[Be 95] Beltiukov, A.P. (1995) Intuitionistic Theories with Realizability in Subrecursive Classes. Forthcoming

[BBT 95] Berardi, S., M. Bezem, T. Coquand. (1995) On the computational content of the Axiom of Choice. *Preprints of Dept. Phil. Utrecht University.*

[BS 95] Berger, U., H, Schwichtenberg (1995) Program development by proof transformation. In H. Schwichtenberg (ed.) *Proof and Computation.* Springer Verlag, Berlin. 1-45.

[BS 95*] Berger, U., H, Schwichtenberg (1995) The greatest common divisor: a case study for program extraction from classical proofs. Forthcoming.

[B 56] Beth, E.W. Semantic construction of intuitionistic logic. *Kon.Ned. Ak. Wet. Afd. Let. Med. 19/11*, 357-388.

[CU 93] Cook, S., A. Urquhart (1993) Feasible interpretations of feasibly constructive arithmetic. *APAL* 63, 103-200.

[CD 62] Crossley, J., M. Dummett (1962) *Formal Systems and Recursive Functions.* North-Holland, Amsterdam.

[CF 58] Curry, H.B., R. Feys (1958) *Combinatory Logic*, North Holland, Amsterdam Section E.

[DG 71] Dalen, D. van, C. Gordon (1971) Independence problems in subsystems of intuitionistic arithmetic. *Ind. Math.* 33, 448-456.

[D 74] Dalen, D. van (1974) A model for HAS. A topological interpretation of second order intuitionistic arithmetic with species variables.*Fund. Math.* 82,167-174.

[D 78] Dalen, D. van (1978) An interpretation of intuitionistic analysis., (with) *Annals Math.Logic* 13,1-43.

[D 84] Dalen, D. van (1984) How to glue analysis models, *JSL* (49), 1339-1349.

[D 86] Dalen, D. van (1986) Glueing of Analysis Models in an Intuitionistic Setting. (with) *Studia Logica* 45, 181-186.

[DV 88] Dalen, D. van, F.J. de Vries (1988) Intuitionistic Free Abelian Groups, *Zeitschr. f. math. Logik und Grundlagen d. Math.* 34, 3-12.

[D 95] Dalen, D. van (1995) Hermann Weyl's Intuitionism. *The Bulletin of Symbolic Logic* 1, 145-169.

[D 96] Dalen, D. van (1996) 'Outside' as a primitive notion in constructive projective geometry. *Geometrica Dedicata*, 60, 107-111.

[D 95] Damnjanovic, Z.(1995) Minimal Realizability of Intuitionistic Arithmetic and Elementary Analysis. *JSL* 60, 1208-1241.

[Du 75] Dummett, M. (1975) The philosophical basis of intuitionistic logic. In [RS 75] 5-40. Also in [Du 78]

[Du 78] Dummett, M. (1978) *Truth and other Enigmas*, Duckworth, London.

[G 81] Gabbay, D. (1981) *Semantical Investigations in Heyting's Intuitionistic Logic.* Reidel, Dordrecht.

[GG 86] Gabbay, D., F. Guenthner (eds.) (1986) *Handbook of Philosophical Logic III.* Kluwer, Dordrecht.

[Gal 95] Gallier, J. (1995) On the Correspondence between proofs and λ-terms. In [Gr 95], 55-138.

[GLT 89] Girard, J.-Y., Y. Lafont, P. Taylor (1989) *Proofs and Types.* Cambrideg University Press. Cambridge.

[G 95] Girard, J.Y. (1995) Linear Logic: A Survey in [G 95], 193-255.

[Gr 95] Groote, Ph. de, (1995) *The Curry-Howard Isomorphism.* Academia. Louvain-la Neuve.

[H 27] Heyting, A. (1927) Die Theorie der linearen Gleichungen in einer Zahlenspezies mit nicht kommutativer Multiplikation. *Math. Ann.* 98, 465-490.

[H 34] Heyting, A. (1934) *Mathematische Grundlagenforschung. Intuitionismus. Beweistheorie.* Springer Verlag, Berlin.

[H 41] Heyting, A. (1941) Untersuchungen über intuitionistische Algebra. *Verh. Ned. Ak. Wet. 18, no.2*, pp. 36

[HM 84] Hoeven, G. van der, I. Moerdijk (1984) Sheaf models for choice sequences. *APAL* 217, 63-107.

[Ho 80] Howard, W. (1980) The Formulae-as-Types Notion of Construction. In [SH 80], 479-490.

[Hy 82] Hyland, J.M.E. (1982) The effective topos in [TD 82], 165-216.

[K 45] Kleene, S.C. (1945) On the interpretation of intuitionistic number theory *JSL* 10, 109-124.

[K 73] Kleene, S.C. (1973) Realizability, a retrospective survey. In [MR 73].

[Kr 65] Kreisel, G. (1965) Mathematical Logic. In Lectures on Modern Mathematics III (ed. T.L. Saaty). Wiley & Sons. New York.

[K 62] Kripke, S. (1962) Semantical Analysis of intuitionistic logic I. In [CD 62], 92-130.

[L 95] Lipton (1995) Realizability, Set Theory and Term Extraction. In [G 95] 257-364.

[M 71] Markov, A.A. (1971) On Constructive Mathematics. *Tr. Mat. Inst. Steklov* 67, 8-14. Also *Am. Math. Soc. Transl. II Ser.* 98(1971), 1-9.

[MM 92] MacLane, S., I. Moerdijk (1992) *Sheaves in Geometry and Logic* Springer Verlag. Berlin.

[M 84] Martin-Löf, P. *Intuitionistic Type Theory.* Bibliopolis, Napels.

[MR 73] Mathias, A., H. Rogers Jr. (1973) *Proceedings of the Cambridge Summer School in Mathematical Logic.* Springer Verlag, Berlin.

[M 86] McCarty, D.C. (1986) Realizability and recursive set theory. APAL 32, 11.194.

[M 91] McCarty, D.C. (1991) Incompleteness in Intuitionistic Metamathematics. *Nptre Dame J. of Formal Logic* 32, 323-358.

[M 82] Moerdijk, I. (1982) Glueing topoi and higher-order disjunction and existence. In [TD 82], 359-376.

[M 95] Moerdijk, I. (1995) A model for intuitionistic non-standard arithmetic. *APAL* 73, 37-52.

[Mos 73] Moschovakis, J.R. (1973) A topological interpretation of second-order intuitionistic arithmetic. *Comp. Math.* 26, 261-276.

[O 94] Oosten, J. van (1994) Axiomatizing higher-order Kleene realizability. *APAL* 70, 87-111.

[Pa 95] Palmgren, E. (1995) A constructive approach to non standard analysis. *APAL* 73, 297-325.

[Pi 90] Pitts, A.M. (1990) Polymorphism is set theoretic, constructively. In *Logical Foundations of Functional Programming.* Reading, M.A. Addison-Wesley.

[Pl 95] Plato, J. von 1995) The axioms of constructive geometry. *APAL* 76, 169-200.

[Pr 77] Prawitz, D. (1977) Meaning and proofs: on the conflict between classical and intuitionistic logic. *Theoria* 43, 1-40.

[RS 63] Rasiowa, H., R. Sikorski (1963) *The mathematics of metamathematics.* PWN. Warsaw.

[RS 75] Rose, H.E., J. Shepherdson (eds.) (1975) *Logic Colloquium 1973*, North-Holland, Amsterdam.

[S 68] Scott, D.S. (1968) Extending the topological interpretation to intuitionistic analysis. *Comp. Math.* 20, 194-210.

[S 70] Scott, D.S. (1970) Extending the topological interpretation to intuitionistic analysis, II. In [Kino, Myhill, Vesley], 235-255.

[SH 80] Seldin, J.P., J.R. Hindley. (1980) *To H.B. Curry: Essays on Combinatoric Logic, Lambda Calculus and Formalism.* Ac. Press.

[Sm 73] Smorynski, C.A. (1973) Applications of Kripke Models in [T 73], 324-391.

[Sm 82] Smorynski, C.A. (1982 Non-standard models and constructivity. In [TD 82], 495-464.

[Su 86] Sundholm, G. (1986) Proof Theory and Meaning. In [GG 86] 471-506.

[T 92] Troelstra, A.S. (1992) Realizability. *ILLC Prepublication Series* ML-92-09 University of Amsterdam.

[T 73] Troelstra, A.S. (1973) *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis.* SLNM 344. Springer Verlag, Berlin.

[TD 82] Troelstra, A.S., D. van Dalen (1982) *The L.E.J. Brouwer Centenary Symposium.* North-Holland, Amsterdam.

[TD 88] Troelstra, A.S., D. van Dalen, (1988) *Constructivism in Mathematics. 1,2* , North-Holland. Amsterdam.