# Computational Content of Classical Logic

*Thierry Coquand*

## Introduction

This course is an *introduction* to the research trying to connect the proof theory of classical logic and computer science. We omit important and standard topics, among them the connection between the computational interpretation of classical logic and the programming operator callcc[1].

Instead, here we put the emphasis on actual mathematical examples. We analyse the following questions: what can be the meaning of a non-effective proof of an existential statement, a statement that claims the existence of a finite object that satisfies a decidable property? Is it clear that a non-effective proof has a meaning at all? Can we always say that this proof contains implicitly, if not explicitly, some effective witness? Is this witness unique? By putting the emphasis on actual mathematical examples, we follow Gentzen who founded natural deduction by analysing concrete mathematical examples, like Euclid's proof of the infinity of prime numbers.

We present general *methods* that can be used to compute effectively such witnesses. The three methods we shall analyse are[2]

1. The negative translation. This is a quite natural translation of classical logic in intuitionistic logic, which is both simple and powerful.

2. A game-theoretic interpretation of classical logic, which is a suggestive reformulation of Gentzen-Novikov's sequent calculus, and may be in some cases more convenient than negative translation.

3. Use of formal topology. It consists of realising some conditions in a topological model. In some cases, it is possible then to realise these conditions effectively, while the "absolute" realisation of these conditions is impossible. Though the extent of this method is not completely elucidated yet, it has given unexpected results in difficult cases where the negative translation cannot be used. (We present among applications a new proof of Herbrand's theorem, and an analysis of one proof of van der Waerden's theorem on arithmetical progressions.)

[1] See the references at the end of part I.

[2] A method that is not analysed here is the "no conterexample" interpretation, due to Kreisel, and explained in detail in Girard's book "Proof Theory and Logical Complexity", Bibliopolis.

# 1 The Negative Translation

Two systems that we analyse are Peano Arithmetic, written PA, and Heyting Arithmetic, written HA.[3]

The system HA is a theory in first-order intuitionistic logic. We add function symbols for primitive recursive functions, and the axioms are the defining equations of these equations, and the induction schema. See [TroeDal] and [Gentzen69] for the complete presentation of this formal system.

The system PA can be defined as the system HA where we add the schema $\neg A \vee A$ or, equivalently, $\neg\neg A \Rightarrow A$. We recall that $\neg\phi$ can be seen as an abreviation for $\phi \Rightarrow\perp$ .

## 1.1 Markov's rule

Markov's principle is the schema, for a quantifier-free formula $\phi$

$$\neg\neg\exists x\ \phi \Rightarrow \exists x\ \phi \qquad (MP).$$

More generally, we can consider the schema

$$[\forall x\ [\phi \vee \psi]], [\neg\forall x\ \phi] \Rightarrow [\exists x\ \psi], \qquad (MP')$$

for arbitrary formulae $\phi$ and $\psi$. This schema implies $(MP)$ for a decidable formula $\phi$ by taking $\psi = \neg\phi$.

This schema is *not* derivable.

We should make the meaning of this last sentence more precise, especially the meaning of the word "schema". An example of a intuitionistically valid derivable schema is

$$\neg\exists x\phi \Rightarrow \forall x\neg\phi,$$

and by this, we mean that it is provable by the laws of intuitionistic logic if $\phi$ is $P\ x$, where $P$ is a new predicate variable. Indeed, the formula

$$\neg\exists x P\ x \Rightarrow \forall x\neg P\ x,$$

is provable from the elimination rule for existential quantification, recalling that $\neg\ \phi$ is defined as $\phi \Rightarrow\perp$ . The claim is that such a justification is not possible for the schema $(MP')$.

There are at least two proofs of this fact, both interesting. The first one uses modified realizability (and was the motivation for the introduction of this notion [Kreisel59]). The second one uses topological, or Beth, models. Both are in the exercises.

[3] These names are quite misleading because in the form they are now presented, both systems are expressed in first-order logic, while both Peano and Heyting formulated their systems using higher-order logic, i.e. with quantification over variables ranging over properties.

It can appear at first counter-intuitive that this principle does not hold intuitionistically, and this may seem a kind of incompleteness of the system HA. It seems that we do have an algorithm that will compute a witness: test successively $\phi\ 0$ or $\psi\ 0$, $\phi\ 1$ or $\psi\ 1 \ldots$ until one finds a value $n_0$ such that $\psi\ n_0$. Such an algorithm is not accepted intuitionistically, because we don't have any justification that this search will stop (only that it is impossible that it goes on forever).

However, if Markov's principle is not derivable, it is valid as a *rule*. By this we mean the following. Given a decidable formula $\phi$, if $\neg\forall x.\neg\phi$ is provable in HA, then $\exists x.\phi$ is provable in HA.

We will prove this for an atomic formula $\phi$. (The case of a quantifier-free formula is an exercise.) Notice however that if $\phi$ is decidable, we can always consider an extension of HA with a new predicate variable $P$ such that $P\ x$ is equivalent to $\phi$. (In exercise 5, it is shown how to reduce the case of a decidable formula to a quantifier free formula without extending HA.)

One can read this principle as: if $\exists x\phi$ is provable classicaly, then it is provable intuitionistically. In this form, this was shown by Novikov [Novikov43], and implicitly by Gentzen. An elegant proof is given by Friedman [Friedman78], and it is this proof that we present. The analogy with the monad of exceptions, used in functional programing, is striking, and we present a small example that illustrates this analogy.

## 1.2 Closure under Markov's rules

We present Friedman's proof that if $\neg\neg\exists x\ \phi$ is provable in HA, then so is $\exists x\ \phi$, where $\phi$ is quantifier free. This relies on the following translation:

- $P^*$ is $P \vee A$, if $P$ is atomic,
- $(B \vee C)^*$ is $B^* \vee C^*$,
- $(B \wedge C)^*$ is $B^* \wedge C^*$,
- $(B \Rightarrow C)^*$ is $B^* \Rightarrow C^*$,
- $(\forall x\ B)^*$ is $\forall x\ B^*$,
- $(\exists x\ B)^*$ is $\exists x\ B^*$,
- $\perp^*$ is $A$,

where $A$ is the formula $\exists x\ \phi$.

**Proposition:** If $B$ is provable in HA, then so is $B^*$.

This is direct.

**Remark:** If $B$ is $\neg\forall x\ \neg\phi$, then $B^*$ is equivalent to $A$.

**Theorem:** If $\neg\forall x\ \neg\phi$ is provable in HA (with $\phi$ quantifier free), then so is $\exists x\ \phi$.

**Proof:** Let $B$ be $\neg\forall x\ \neg\phi$. If $B$ is provable in HA, then so is $B^*$ by the proposition. By the remark, $B^*$ is equivalent to $\exists x\ \phi$, and hence $\exists x\ \phi$ is provable. $\square$

This translation is strongly reminiscent of the use of the exception monad [Moggi,SpiWad90] used in functional programming. The existential formula $A$ corresponds to a fixed data type of error messages, and the operation on types is $T\ X\ =\ X + A$, which corresponds to the translation of atomic formulae.

Notice that we don't start from a classical proof of $\exists x.\phi$. Only an intuitionistic proof that it is impossible not to have an $x$ such that $\phi$ holds. The next section will show how to transform a proof of $\exists x.\phi$ in PA into a proof of the same statement in HA.

## 1.3 Negative Translation

This translation can be traced back to Kolmogorov. A propositional form of this result was then stated by Glivenko, and it is not clear how much this has influenced the work of Gödel, Gentzen and Bernays. The references can be found in Gödel's collected work [God86]. The form stated in Kolmogorov is quite strong, since he claimed that, via the double negation translation, one can establish that a finitary result proved with the principle of excluded middle can be proved without using this principle. This strong form is still open however, and, as we shall see, the negative translation does not work in the presence of the Axiom of Choice.

The intuition behind this translation can be described as follows. There is a difference between the connective $\wedge$ and universal quantification on one side, and on the other side, disjunction and existential quantification. If a classical mathematician claims to have a proof of $A \wedge B$, he claims that he has a proof of $A$ and a proof of $B$, like in intuitionistic logic. But if he claims to have a proof of $A \vee B$, he may claim only to have deduced a contradiction from the hypothesis that neither $A$ not $B$ hold. In the same way, if he claims to have a proof of $\exists x\ A$, he may mean only that he has arrived at a contradiction from the hypothesis that $A$ never holds.

Notice that the connectives $\exists$ and $\vee$ have a special status. This point is discussed in Gentzen's collected works [Gentzen69].

**Theorem:** If $\exists x\ \phi$ is provable in PA (with $\phi$ decidable), then it is provable in HA.

This theorem does not hold if $\phi$ is not a decidable formula. It may even happen that $\exists x\ \phi$ is provable in $\mathsf{PA}$, but that $\phi(n_0)$ is not provable in $\mathsf{PA}$ for any given numeral $n_0$ (see the exercises).

The proof of the theorem relies on the following translation:

- $P^*$ is $\nabla P$, if $P$ is atomic,
- $(B \wedge C)^*$ is $B^* \wedge C^*$,
- $(B \Rightarrow C)^*$ is $B^* \Rightarrow C^*$,
- $(\forall x\ B)^*$ is $\forall x\ B^*$,
- $(B \vee C)^*$ is $\nabla\ (B^* \vee C^*)$,
- $(\exists x\ B)^*$ is $\nabla(\exists x\ B^*)$,
- $\perp^*$ is $A$,

where $A$ is the formula $\exists x\ \phi$, and $\nabla\ B$ is $(B \Rightarrow A) \Rightarrow A$.

**Proposition:** If $B$ is provable in $\mathsf{PA}$, then $B^*$ is provable in $\mathsf{HA}$.

The proof is direct by induction on the proof of $B$. We comment rather on cases where this proposition *cannot* be applied. A good example is the fundamental theorem if algebra on the existence of roots. In this case, it happens to be possible to compute effectively the roots of a given polynomial, but this does not follow directly from a general meta-theorem. But the form of the statement "there exists a root $x_0$" of a given polynomial $P$ is not, contrary to what it may seem, purely existential. Indeed, the statement $P(x_0) = 0$ is not decidable, but a universally quantified statement. To prove constructively this existence statement, one possibility is to prove first that there exists a rational $x_1$ such that $P(x_1)$ is "small", and then to use Newton's method to compute a zero of $P$ from $x_1$.

The following proposition gives an example where a computational content is not possible. If $f$ is a continuous function over $[0,1]$ and $f(0) < 0,\ f(1) > 0$, then there exists $x$ such that $f(x) = 0$. This holds classically, but it is not possible to extract an algorithm parametric in $f$ that computes a root of $f$ [TroeDal].

In functional programming, there is a monad closely connected to this translation. Given a data type $A$, one defines the "continuation monad" by $T\ X\ =\ (X {\rightarrow} A) {\rightarrow} A$. Notice that the operator $\nabla$ on propositions can be seen as a modal operator and satisfies the law corresponding to the laws of a monad [SpiWad90].

- $B \Rightarrow \nabla\ B$,
- $\nabla\ B$ and $B \Rightarrow \nabla\ C$ entail $\nabla C$.

Wadler [SpiWad90] has shown how to represent in an elegant way non functional operations in a purely functional programming language. This suggests that it should be possible to "simulate" classical reasoning by working in an intuitionistic framework with such a modality. The next section presents such a simulation on a simple example, due to U. Berger and H. Schwichtenberg.

## 1.4 Monads on Propositions

The goal of this section is to show that we can use monads as well on propositions. They can be used to simulate "impure features", here the use of excluded middle, in a pure Type Theory.

Here is the reasoning we want to simulate. Given a function $f : \mathsf{N}\rightarrow\mathsf{N}$, with a proof $h_1 : \forall x \exists y\ x < f\ y$, and given $x_0 : \mathsf{N}$ with a proof $h_2 : f\ 0 \leq x_0$, we want to find $n$ such that $f\ n \leq x_0$ and $x_0 < f\ (S\ n)$. That is we want to prove constructively $P = \exists\ n.f\ n \leq x_0 \wedge x_0 < f\ (S\ n)$. (This example is due to U. Berger and H. Schwichtenberg.)

Here is a classical proof (impure). Suppose $\neg\ P$, that is

$$h_3 : \forall n\ f\ n \leq x_0 \Rightarrow x_0 < f\ (S\ n) \Rightarrow \perp$$

we prove

$$\forall n\ f\ n \leq x_0 \qquad\qquad (*)$$

by induction on $n$.

For $n = 0$, it holds by $h_2$.

If $f\ n \leq x_0$, we cannot have $x_0 < f(Sn)$ by $h_3$, hence $f\ (S\ n) \leq x_0$.

But $(*)$ contradicts $h_1$, hence by excluded middle, we have $P$.

We simulate this impure reasoning by using the monad/modality $\nabla$ : $\mathsf{Set}\rightarrow\mathsf{Set}$ defined by $\nabla\ X = X \vee P$.

Notice that we have $\mathsf{unit} : X \Rightarrow \nabla\ X$ and $\mathsf{bind} : \nabla\ X \Rightarrow [X \Rightarrow \nabla\ Y] \Rightarrow \nabla\ Y$. The following rule is derived from $\mathsf{bind}$ by induction

$$\frac{\nabla\ (A\ 0) \qquad A\ n \Rightarrow \nabla\ (A\ (S\ n))}{\nabla\ (A\ n)} \qquad (**).$$

This holds for a general monad.

For this particular monad we have furthermore

$$lem_1 : \forall X \forall n\ f\ n \leq x_0 \Rightarrow x_0 < f\ (S\ n) \Rightarrow \nabla\ X$$

and

$$lem_2 : \forall X\ \neg X \Rightarrow \nabla\ X \Rightarrow P$$

Now, we prove

$$\forall n\ \nabla\ (f\ n \le x_0)$$

by using the rule $(**)$.

For $n = 0$, using $h_2$ and unit.

If $f\ n \le x_0$, then there are two cases. If $f\ (S\ n) > x_0$, we have $\nabla\ (f\ (S\ n) \le x_0)$ by $lem_1$ and if $f\ (S\ n) \le x_0$, we have $\nabla\ (f\ (S\ n) \le x_0)$ by unit.

This reasoning follows closely the classical reasoning.

We can now compute $y_0$ such that $x_0 < f\ y_0$ by $h_1$. Since we have

$$\nabla\ (f\ y_0 \le x_0)$$

we deduce $P$ by $lem_2$.

What is the extracted program behind this reasoning?

In Gofer/Haskell [Augustsson], we would introduce

```
M a = Ok a | Exit Int
```

and program

```
exitM :: Int -> Ok a
exitM n = Exit n

g :: Int -> M ()

g 0 = unitM ()

g (n+1) =
g n `bindM` \ _ ->
if x_0 < f (n+1)
   then exitM n
   else unitM ()
```

This program can be seen to be the Gofer version of our monadic proof.

The correctness of this program takes the form: if $x_0 < f\ n$, then $g\ n$ will be of the form Exit $p$, with $p < n$ such that $f\ p \le x_0 < f\ (S\ p)$.

## 1.5 Exercises on Part I

1. Show that adding the schema $\neg A \vee A$ or the schema $\neg\neg A \Rightarrow A$ leads to the same theory.

2. We have $[\neg\neg A \wedge \neg\neg B] \Rightarrow \neg\neg[A \wedge B]$. Notice that there are two ways, not symmetric in $A$, $B$ to prove this.

   Deduce from this that $\neg\neg A$ is provable intuitionistically iff $A$ is provable classically for propositional logic.

   For infinite conjunction, we need Spector's "double negation shift" $\bigwedge \neg\neg A_i \Rightarrow \neg\neg \bigwedge A_i$. Show that the schema $\forall x\ \neg\neg A \Rightarrow \neg\neg\forall x\ A$ does not hold intuitionistically. (Hint: show otherwise that the negative translation of the Axiom of Choice would be provable and use the results of Part III.)

3. Using a Gödel sentence, give an example of a formula $\phi$ such that $\mathsf{PA}$ proves $\exists x\ \phi$, but $\phi(n_0)$ is not provable in $\mathsf{PA}$ for any given numeral $n_0$. (Hint: let $\psi$ a decidable formula such that $G = \forall n\ \neg\ \psi$ is not provable in $\mathsf{PA}$ but $\psi[n_0]$ holds for no given numeral $n_0$. Consider the formula $\exists n\ [\psi \vee G]$.)

4. A *positive formula* is a formula built from atomic formula, existential quantification, finite conjunction and disjunction. A *geometric formula* is a formula of the form $\forall x_1, \ldots, x_n\ [\phi \Rightarrow \psi]$ where $\phi$ and $\psi$ are positive formulae. Finally, a *geometric theory* is a set of geometric formulae. Prove that if a geometric formula is provable in $\mathsf{PA} + T$ where $T$ is geometric, then it is provable in $\mathsf{HA} + T$.

5. Extend the proof of closure under Markov's rule to the case of quantifier-free formula. (G. Huet) Define a "semantical" negative translation such that $\phi^*$ is $\nabla\phi$ if $\phi$ is provably decidable in $\mathsf{HA}$, that is $\mathsf{HA} \vdash \phi \vee \neg\phi$. Use this to prove that if $\exists x\ \phi$ is provable in $\mathsf{PA}$ and $\phi$ is decidable in $\mathsf{HA}$, then $\exists x\ \phi$ is provable in $\mathsf{HA}$. For another proof, see Troelstra and van Dalen, Constructivism in Mathematics, volume I, exercise 4.4.8.

6. (U.Berger and H. Schwichtenberg) Let $f$ be a function such that the formula
$$\forall x\ \exists y\ x < f\ y$$
   is provable in $\mathsf{HA}$. Prove in $\mathsf{PA}$
$$\forall x\ [f\ 0 \leq x \Rightarrow \exists y\ f\ y \leq x < \ f\ (y+1)].$$
   and notice that the natural non-constructive proof of this statement is actually a proof of
$$\forall x\ [f\ 0 \leq x \Rightarrow \neg\neg\exists y\ f\ y \leq x < \ f\ (y+1)].$$
   in $\mathsf{HA}$. What is the algorithm implicit in this non-constructive argument? Given $x_0$, apply Friedman's translation by considering the modality $\nabla\ A = A \vee P$, where $P$ is the proposition $\exists y\ f\ y \leq x_0 < \ f\ (y+1)]$.

7. (U.Berger and H. Schwichtenberg) Same exercise as the previous one, with the following problem: given a decidable property $\phi$ on binary tree, and a binary tree that satisfies $\phi$, find a binary tree that satisfies $\phi$ such that no proper subtree satisfies $\phi$.

8. Markov's principle is not derivable in $\mathsf{HA}$ (of course, it holds directly in $\mathsf{PA}$, why?). One way to see this is by modified realizability [Kre59]: we interpret proofs of $\mathsf{HA}$ as programs defined by primitive recursion, and we see that, if Markov's principle was provable, we could solve the halting problem. This was actually Kreisel's motivation for introducing the notion of modified realizability. The other way is by building a boolean model of $\mathsf{HA}$ in which Markov's principle does not hold.

   For this, consider the boolean algebra $\mathsf{B}$ freely built on countably many propositional letters $A_0,\ A_1,\ldots$ Propositions of $\mathsf{HA}$ are interpreted as ideals of this boolean algebra. We have $\neg\neg \bigvee A_n$, because 0 is the only element of $\mathsf{B}$ less or equal than all $\neg A_n$, but $\bigvee A_n$, which is the ideal generated by all the $A_i$, is not the unit ideal.

9. Let $f$ be a parameter, ranging over functions from integers to integers. We can prove classically

   $$[\exists x \forall y\ f(y) \leq x] \vee [\forall x \exists y\ x < f(y)]$$

   and deduce from each case

   $$\exists x_1, x_2, x_3\ [x_1 < x_2 < x_3 \wedge f(x_1) \leq f(x_2) \leq f(x_3)].$$

   For some concretely given $f$, compute witnesses for this statement using Friedman's method.

10. (G. Stolzenberg) Let $f$ be a parameter, ranging over functions from integers to booleans. Give a proof in natural deduction of the "infinite box principle"

    $$\forall x_0 \exists y_0 [x_0 \leq y_0 \wedge f(y_0) = 0] \vee \forall x_1 \exists y_1 [x_1 \leq y_1 \wedge f(y_1) = 1].$$

    Use this to prove classically

    $$\exists a \exists b\ [a < b \wedge f(a) = f(b)]$$

    using as lemmas (that are valid intuitionistically)

    $$\forall x_0 \exists y_0 [x_0 \leq y_0 \wedge f(y_0) = 0] \Rightarrow \exists a \exists b\ [a < b \wedge f(a) = f(b)],$$

    and

    $$\forall x_1 \exists y_1 [x_1 \leq y_1 \wedge f(y_1) = 1] \Rightarrow \exists a \exists b\ [a < b \wedge f(a) = f(b)].$$

Use Gödel-Gentzen-Friedman translation in order to transform these proofs into a functional $F(f) = (a, b)$ that, given $f$, computes a pair $(a, b)$ such that $a < b$ and $f(a) = f(b)$. Is this functional the same as the one that computes $f(0)$ $f(1)$ and $f(2)$ and looks for two equal values among these three?

11. A "classical" example of a non-constructive proof is the following argument for the existence of two irrational numbers $x$ and $y$ such that $x^y$ is rational. Consider $a^a$ for $a^2 = 2$. Classically, either it is rational, and we can then take $x = y = a$, or it is irrational and we can take $x = a^a$, and $y = a$.

    Since the statement proved is *not* a purely existential statement about "concrete" objects, but about real numbers, it is not possible a priori to give an effective meaning to this reasoning.

    Compare this with the following argument: for each $x$ in $[2, 3]$ there exists $y = g(x) > 0$ such that $x^y = 2$. Notice that $g$ is one-to-one. Consider all pairs $(x, g(x))$ such that $x$ is irrational. There are uncountably many such pairs. Hence, using the fact that $g$ is one-to-one, there are uncountably many pairs such that both $x$ and $g(x)$ are irrational (suggested by M. Hofmann). Give an effective version of this argument (Hint: the function $g$ is continuous. Enumerate all rationals $u_k$ and build a nested sequence of rational intervals $I_k$ such that both $I_k$ and $g(I_k)$ contains no $u_j$ for $j < k$.)

## 1.6 References

[Augustsson] L. Augustsson. "Haskell B. user's manual." available over WWW from hhtp://www.cs.chalmers.se:80/pub/haskell/chalmers.

[God86] K. Gödel *Collected Works.* Oxford University Press. Volume I and II.

The formulation of PA and HA: can be traced back to Herbrand and Gödel, see the introduction of Gödel's article on negative translation by Troelstra in the volume I. Herbrand's system and Gentzen's system were *open* systems, very much like Martin-Löf's Intuitionistic Type Theory.

[Berg93] U. Berger and H. Schwichtenberg "Program Development by Proof Transformation." Proof and Computation, proceeding of the Marktoberdof Summer School 1993, NATO ASI Series.

Contains a description of analysis of classical proofs on a machine, and some examples of pruning.

[TroeDal] A.S. Troelstra and D. van Dalen *Constructivism in Mathematics.* Volume I, North-Holland.

Interesting historical introduction, and a lot of nice exercises. Highly recommended.

[Kreisel59] G. Kreisel "Interpretation of analysis by means of constructive functionals." In A. Heyting ed. *Constructivity in Mathematics*, North-Holland.

Among other things, contains the first mention of modified realisability, used to show that Markov's principle is not valid in HA.

[Friedman78] H. Friedman, "Classically and intuitionistically provably recursive functions," in Springer Lecture Notes in Computer Science, Volume 669.

Contains an incredibly easy and clear proof of closure under Markov's rule and a proof that if an existential statement is provable in PA, then it is provable in HA. As an application a function is provably recursive in PA iff it is so in HA. This can be extended to stronger systems, but it is yet unknown for systems that combine Excluded Middle and the Axiom of Choice.

[Novikov43] P.S. Novikoff "On the consistency of a certain logical calculus." Matematiceskij sbornik (Recueil Mathématique) T. 12 (54), pp. 230-260.

Contains an early proof of closure under Markov's rule.

[Gentzen69] G. Gentzen *Collected Works.* M.E. Szabo ed., North-Holland.

Presents a version of the negative translation (discovered about the same time as Gödel's). The introduction of the first paper on consistency proofs for classical arithmetic contains a deep analysis of the difference between the "actualist" (non-effective) and the "intuitionistic" (effective) interpretation of logical connectives.

[Moggi] E. Moggi "Notions of Computation and Monad", Information and Computation, vol. 93, p. 55-62, 1991.

Shows the relevance of the notion of monads in structuring the denotational description of programming languages.

[SpiWad90] P. Wadler "The essence of functional programming", in POPL 92.

M. Spivey "A functional theory of exceptions", Science of Computer Programming 14, 1990.

Presents an elegant way of simulating exceptions, and other "imperative features" in a pure functional programming language. This suggests that similar techniques could be applied to proof systems, and that we can simulate "non-effective features" in a pure intuitionistic system.

[deGroot95] Ph. de Groote "A Simple Calculus of Exception Handling." In proceeding of TLCA 95, LNCS 902.

Presents a logical analysis of ML exceptions. Furthermore, it contains an extended bibliography of related works.

Here are some comments on this reference list.

One paper by Barbanera and Berardi contains another way to extract witnesses, presented in Prawitz's book on Natural Deduction.

The Ph. D. thesis of Ch. Murthy presents the connection between Friedman's translation and CPS transformation.

The paper of T. Griffin started the connections between analysis of classical proofs, and control operators.

The papers of M. Parigot contain an elegant generalisation of the $\lambda$-calculus, called $\lambda\mu$-calculus, that extends in some way the Curry-Howard correspondence between proofs and $\lambda$-terms to non-effective proofs. They have references to papers by J.L. Krivine that contain deep remarks about the connection between classical logics and imperative features.

The paper by J.Y. Girard contains, among other things, an optimised version of the translation of H. Friedman, that is analysed in the LICS 91 paper of Ch. Murthy.

[Weyl] H. Weyl "Ueber die neue Grundlagenkrise der Mathematik", Mathematische Zeitschrift, 10, 1921.

# 2 Sequent Calculus

In this second part, we present another way of making constructive sense of classical reasoning: the sequent calculus. First, we analyse the formulation as it appears in Gentzen first proof of consistency for classical arithmetic. Next, we present a simplified version of Novikov's calculus, written with Hugo Herbelin, and a game-theoretic interpretation of this calculus.

## 2.1 Gentzen's calculus

### 2.1.1 Presentation of the system

The language is the same as in $\mathsf{HA}, \mathsf{PA}$, but Gentzen restricts it to the fragment defined by the connectives $\forall, \wedge, \neg$. The logic is represented by Natural Deduction with sequents of the form $\Gamma \vdash A$ where $\Gamma$ is a set of formulae. We write $\Gamma, A$ for $\Gamma \cup \{A\}$, and $\Gamma, \Delta$ for $\Gamma \cup \Delta$. The intuitionistic logical rules are

- if $A$ is in $\Gamma$ then $\Gamma \vdash A$,
- if $\Gamma \vdash A \wedge B$ then $\Gamma \vdash A$ and $\Gamma \vdash B$,
- if $\Gamma \vdash A$ and $\Gamma \vdash B$ then $\Gamma \vdash A \wedge B$,
- if $\Gamma \vdash A(x)$ and $x$ is not free in $\Gamma$ then $\Gamma \vdash \forall x\ A(x)$,
- if $\Gamma \vdash \forall x\ A(x)$ then $\Gamma \vdash A(t)$ for all terms $t$,
- if $\Gamma, A \vdash \perp$ then $\Gamma \vdash \neg A$,
- if $\neg A$ is in $\Gamma$, and $\Gamma \vdash A$ then $\Gamma \vdash \perp$ .

There are two remaining rules. The induction rule is: from $\Gamma \vdash F(1)$ and $\Delta, F(a) \vdash F(a+1)$, follows $\Gamma, \Delta \vdash F(t)$, provided $a$ fresh w.r.t. $\Gamma, \Delta, F(1), F(t)$. Finally, the double negation rule is that $\Gamma \vdash A$ follows from $\Gamma \vdash \neg\neg A$.

Notice that it is a finitary inductive definition of $\vdash$ . (See [Aczel78] for an introduction to the notion of inductive definition.)

### 2.1.2 First Analysis

As analysed by Gentzen, the more problematic rule is the double negation rule that $\Gamma \vdash A$ follows from $\Gamma \vdash \neg\neg A$. Without this rule, we have a formalisation of the intuitionistic system $\mathsf{HA}$, and this system has a direct intuitionistic meaning.

Gentzen has then an interesting discussion on "finitary" versus "infinitary", or non-effective interpretation of this system. He notices that the rules can be justified by a non-effective interpretation.

### 2.1.3 Non-standard interpretation

Gentzen then gives another, "non-standard" effective interpretation of the system. "The propositions of actualist mathematics seem to have a certain utility, but no *sense*. The major part of my consistency proof, however, consists precisely in *ascribing a finitary sense* to actualist propositions." This gives yet another computational content of classical proofs. This computational content is described by Gentzen as a *non-deterministic* algorithm. I will describe it as an *interactive* algorithm.

### 2.1.4 Reduction rule on sequents

This is an interactive algorithm between the "proof" and an opponent. All the formulae of the sequents are closed, and we can compute the truth value of any atomic statement. The opponent plays as long as the conclusion formula is not atomic, by "reducing" the sequent according to the following rules

- $\Gamma \vdash A \wedge B$ can be reduced to $\Gamma \vdash A$ or $\Gamma \vdash B$,
- $\Gamma \vdash \forall x\ A(x)$ can be reduced to any $\Gamma \vdash A(n_0)$,
- $\Gamma \vdash \neg A$ is reduced to $\Gamma, A \vdash \perp$ .

The interaction stops if the conclusion is atomic and true. If the conclusion is atomic and false, it is the turn of the "proof" to play. The "proof" plays as long as the conclusion is atomic and false, and there is no atomic and false formulae among the antecedant formulae. It plays also by reducing the sequent, in the following way:

- if $A \wedge B$ is in $\Gamma$ then $\Gamma \vdash \perp$ can be reduced to $A, \Gamma \vdash \perp$, or to $B, \Gamma \vdash \perp$,
- if $\forall x\ A(x)$ is in $\Gamma$ then $\Gamma \vdash \perp$ can be reduced to any $A(n_0), \Gamma \vdash \perp$,
- if $\neg A$ is in $\Gamma$ then $\Gamma \vdash \perp$ can be reduced to $\Gamma \vdash A$ (and then it is the opponent turn to play, if the formula $A$ is not atomic and false),
- if a false formula is in $\Gamma$ then the game stops at $\Gamma \vdash \perp$ and the proof wins.

Thus during a play, the proof and its opponent try alternatively to reduce the sequent. The proof tries either to make the end formula atomic and true, or to make one antecedant formula atomic and false.

The finitary interpretation is a "reduction rule", i.e. a strategy for the proof. After finitely many interaction steps, the proof should reach a situation where either there is a true atomic conclusion formula, or there is a false atomic conclusion formula and a false atomic antecedant formula.

A strategy for the proof that achieves this, against any opponent (even if the opponent does not follow any fixed strategy), will be the "finitary meaning" of the sequent.

For instance, $\forall x\ P(x) \vdash \forall x\ P(x)$ has such a finitary meaning, if $P$ is decidable. The strategy is as follows: the opponent has to give a value $x = x_0$ for $x$, and the sequent reduces then to $\forall x\ P(x) \vdash P(x_0)$. If $P(x_0)$ is true, then the game is finished. Otherwise, the proof can play by choosing also the same value $x = x_0$ reducing the sequent to $P(x_0), \forall x\ P(x) \vdash P(x_0)$ where $P(x_0)$ is a false atomic formula.

What is important here is that this strategy is an effective object, though we cannot decide of the truth value of the formula $\forall x\ P(x)$.

Finally, notice that it is the *sequent* itself that is "reduced" by the proof and its opponent; the "reduction" does not concern the proof, which is a strategy for doing this "reduction".

### 2.1.5 What Gentzen proves

Gentzen proves then that any provable sequent has a reduction rule. Since the sequent $\vdash 1 = 2$ has no reduction rule, it will follow that $\vdash 1 = 2$ is not provable.

Notice also that if $\forall x\ \neg P(x) \vdash \perp$ has a reduction rule, then this reduction rule gives us $x_0$ such that $P(x_0)$ holds. So we get that $\exists x\ P(x)$ holds intuitionistically if it is provable in PA. This result is mathematically weaker than Friedman/Dragalin's result, but it is enough for extracting computations from classical proofs.

The key step in the proof is the *cut lemma*: from a reduction rule for $\Gamma \vdash B$ and $\Delta, B \vdash A$, to give a reduction rule for $\Gamma, \Delta \vdash A$.

For instance, this gives an interpretation of the elimination of the double negation.

### 2.1.6 Cut lemma

The cut lemma that provides a reduction rule for $\Gamma, \Delta \vdash A$ given one for $\Gamma \vdash B$ and $\Delta, B \vdash A$ is proved by case analysis of the cut formula $B$.

If $B$ is atomic, if it is true, we can simulate the reduction rule of $\Delta, B \vdash A$, and if it is false, we can simulate the reduction rule of $\Gamma \vdash B$.

The general case is more complicated and we refer the reader to Gentzen's original article or to Bernays' presentation of this proof.

### 2.1.7 Inductive definitions

Instead, we show next how to give an alternative presentation, using generalised inductive definitions instead of talking about interactions.

- If $\Gamma \Rightarrow A(n_0)$ for all $n_0$, then $\Gamma \Rightarrow \forall x\ A(x)$,
- if $\Gamma \Rightarrow A$ and $\Gamma \Rightarrow B$, then $\Gamma \Rightarrow A \wedge B$,
- if $A, \Gamma \Rightarrow \perp$, then $\Gamma \Rightarrow \neg A$,

- if $A$ is atomic and true, then $\Gamma \Rightarrow A$,
- if $\forall x\ A(x)$ is in $\Gamma$, and $A(n_0), \Gamma \Rightarrow \perp$, then $\Gamma \Rightarrow \perp$,
- if $A \wedge B$ is in $\Gamma$, and $A, \Gamma \Rightarrow \perp$ or $B, \Gamma \Rightarrow \perp$, then $\Gamma \Rightarrow \perp$,
- if $\neg A$ is in $\Gamma$, and $\Gamma \Rightarrow A$, then $\Gamma \Rightarrow \perp$,
- if there is a false atomic formula in $\Gamma$, then $\Gamma \Rightarrow \perp$ .

The idea is to embed our finitary system for $\mathsf{HA}$ in this infinitary system, that is to show that if $\Gamma \vdash A$, then $\Gamma \Rightarrow A$. This corresponds to the association of a reduction rule to any provable formula. The proof is direct. The cut lemma will be reformulated as the fact that the cut rule is admissible for this extended calculus. This means that $\Gamma \Rightarrow B$ and $\Delta, B \Rightarrow A$ imply $\Gamma, \Delta \Rightarrow A$. The proof is more involved and consists in a double induction, first in the cut formula $B$ and then in the proofs. We will make this argument precise for a simpler sequent calculus in the next section. What should be emphasised is that the argument in this form is much easier to check than the original argument by Gentzen, or its presentation by Bernays [Bernays].

Notice the similarity between this infinitary system and the intuitionistic truth semantics of $\mathsf{HA}$.

This notion of admissibility has indeed been introduced by Lorenzen, while thinking about Gentzen's consistency proof. See "Einfuehrung in die operative Logik und Mathematik", Springer, 1955, p. 5.

## 2.2 Tait/Novikov calculus

We present a simplification both of Tait's calculus, inspired by a game theoretical analogy between a proof and a winning strategy for a game, and of a calculus presented by Novikov 1943, which contains an elegant proof that if a purely existential statement is provable in classical arithmetic, then it holds intuitionistically.

### 2.2.1 Formulae and validity

The *positive* and *negative* formulae are defined inductively [Aczel78].

- if $A_i$ is a family of negative formulae over a countable set, then $\bigvee A_i$ is a positive formula,
- if $A_i$ is a family of positive formulae over a countable set, then $\bigwedge A_i$ is a negative formula,

We can define inductively the negation of a formula: $\overline{A}$ is $\bigwedge \overline{A_i}$ (resp. $\bigvee \overline{A_i}$) if $A$ is $\bigvee A_i$ (resp. $\bigwedge A_i$). Notice that we can represent the false positive formula by taking $0 = \bigvee A_i$ where $(A_i)$ is the empty family of negative formulae. The negative formula 1 is dually defined as $1 = \bigwedge A_i$ where $(A_i)$ is the empty family of positive formulae. To each negative formula $A$ corresponds a positive formula $[A]$ that we get by considering the family of negative formula with only one element $A$.

The notion of classical validity, as described by Novikoff [Novikoff43], defines inductively when a finite multiset of positive formulae is valid. We shall denote by $L, M, N, \ldots$ such multisets, and write $L, A$ the addition of the positive formula $A$ to the multiset $L$. Similarly we write the addition of the multisets $L$ and $M$ as $L, M$.

The multiset $L, A$, where $A = \bigvee A_i$, is valid if there exists $i_0$ such that $A_{i_0}$ is a negative formula $\bigwedge A_{i_0 j}$ such that, for all $j$, the multiset $L, A, A_{i_0 j}$ is valid.

### 2.2.2 Main properties

In this section, we survey the basic properties of this notion of validity.

**Proposition 1:** If $L$ is a multiset of positive formulae, and $A = \bigvee A_i$ a positive formula, then the multiset $L, A, \overline{A_i}$ is valid.

**Proof:** By induction on the formula $A$. We have $A_i = \bigwedge \overline{A_{ij}}$ and, by induction hypothesis, the multiset $L, A, \overline{A_i}, A_{ij}$ is valid for all $j$. Hence the multiset $L, A, \overline{A_i}$ is valid by definition. □

**Proposition 2:** If $L$ is a valid multiset of positive formulae, and $A = \bigvee A_i$ a positive formula, then the multiset $L, A$ is valid.

**Proof:** Direct by induction on the proof of validity of $L$. □

To simplify the presentation of the proofs, we will say that a multiset $L, M$ is valid because of the $L$ part, if it is valid because $L$ can be written $L', B$ where $B = \bigvee B_j$ is a positive formula such that $L', M, B_{j_0 l}$ is valid for one index $j_0$ and all index $l$.

**Proposition 3:** If $L$ is a multiset of positive formulae, and $A = \bigvee A_i$ a positive formula, then the multiset $L, A, A$ is valid iff $L, A$ is valid.

**Proof:** One direction follows from proposition 2. Conversely, let us prove by induction on the proof of validity of $L, A, A$ that $L, A$ is valid.

This is direct if $L, A, A$ is valid because of the $L$ part.

Otherwise, it is because there exists an index $i_0$ such that $L, A, A, A_{i_0 k}$ is valid for all $k$. By induction hypothesis, $L, A, A_{i_0 k}$ is then valid for all $k$ and hence $L, A$ is valid. □

Notice that for propositions 2 and 3, we did not have to do an induction on formulae, but only on proofs of validity.

**Proposition 4:** If $A = \bigvee A_i$ is such that $L, A$ is valid and $M, \overline{A_i}$ is valid for all $i$, then $L, M$ is valid.

**Proof:** By induction, first on the proposition $A$, then on the proof that $L, A$ is valid. It is direct if $L, A$ is valid because of the $L$ part. If it is valid because there exists an index $i_0$ such that $L, A, A_{i_0 j}$ is valid for all $j$, then by induction hypothesis, we have that $L, M, A_{i_0 j}$ is valid for all $j$. By induction on the formula, we have that $L, M, M$ is valid. By proposition 3, we deduce that $L, M$ is valid. □

This direct inductive proof of the admissibility of cut should be contrasted with the argument of [Tait68], that needs first an inversion lemma.

### 2.2.3 Example

In this section, we want to illustrate on one example that our formalism is well suited for representing proofs in classical arithmetics and for analysing their computational content. The mathematical content of the example may seem trivial, but it has revealed what seems to be a deep problem of symmetry in the operation of cut-elimination or negative interpretation.

Here is the non-constructive argument whose constructive content we shall analyse. Given a function $f$ on integers that takes only the value 0 or 1, there exists $i < j$ such that $f(i) = f(j)$. Either there exists infinitely many 0's in the range of $f$, or infinitely many 1's. In the first case, choose $i, j$ two distinct numbers on which $f$ is 0. In the other case, choose $i, j$ two distinct numbers on which $f$ is 1.

This is a highly nonconstructive proof. It is composed of one main lemma: the function $f$ takes infinitely many times the value 0, or infinitely many times the value 1, and two symmetric lemmas: if the function $f$ takes infinitely many time the value $b$, which can be 0 or 1, then there exists $i < j$ such that $f(i) = f(j)$.

For the translation of this proof in our formalism, we represent each decidable formula as the positive formula 0 if it is false, and the positive formula [1] if it is true.

We define

- $A_n = \bigvee_{m \geq n} .f(m) = 0$,
- $B_n = \bigvee_{m \geq n} .f(m) = 1$,
- $C = \bigvee_{i<j} f(i) = f(j)$.

The main lemma can be seen as stating the validity of $A_{n_0}, B_{n_1}$ for all $n_0, n_1$ and the two other lemmas as stating the validity of $\bigvee \overline{A_n}, C$ and $\bigvee \overline{B_n}, C$.

The validity of $A_{n_0}, B_{n_1}$ is clear by computing $f(\mathsf{max}(n_0, n_1))$.

The validity of $\bigvee \overline{A_n}, C$ can be seen as follows. We prove the validity of the sequent $\overline{A_{0m}}, \bigvee \overline{A_n}, C$ for all $m \geq 0$. This is direct if $f(m) \neq 0$. Otherwise, we show the validity of $\overline{A_{(m+1)m'}}, \overline{A_{0m}}, \bigvee \overline{A_n}, C$ for all $m' \geq m + 1$. This is direct if $f(m') \neq 0$. Otherwise, we have found $f(m) = f(m') = 0$ and $m < m'$, and so we have a witness for the formula $C$.

The validity of $\bigvee \overline{B_n}, C$ is established in the same way.

The following multisets

$$C, \bigvee \overline{A_n} \qquad C, \bigvee \overline{B_n} \qquad A_{n_0}, B_{n_1}$$

are valid.

It follows that $C, C$ and hence $C$ is valid. However, there are at least two ways of computing this proof of $C$.

We can first use proposition 4 on

$$C, \bigvee \overline{A_n} \qquad\qquad A_{n_0}, B_{n_1}$$

getting that $C, B_{n_1}$ is valid for all $n_1$, and then again proposition 4 on

$$C, \bigvee \overline{B_n} \qquad C, B_{n_1}$$

getting that $C, C$ is valid.

The other way is to use proposition 4 on

$$C, \bigvee \overline{B_n} \qquad\qquad A_{n_0}, B_{n_1}$$

getting that $C, A_{n_0}$ is valid for all $n_0$, and then again proposition 4 on

$$C, \bigvee \overline{A_n} \qquad C, A_{n_0}$$

getting that $C, C$ is valid.

As the reader can check, these two ways will give two different witnesses. Which one should be considered as "the" witness contained implicitely in this non-effective proof? Or should we consider that the non-effective proof contains in some mysterious ways both witnesses? This kind of question, while rather fundamental, is surprisingly unexplored.

## 2.3 Game-theoretic Interpretation of Sequent Calculus

The notion of intuitionistic validity

- 1 is valid,
- $\bigvee_i \phi_i$ is valid iff there exists $i_0$ such that $\phi_{i_0}$ is valid,
- $\bigwedge_i \phi_i$ is valid iff $\phi_i$ is valid for all $i$,

has a natural game theoretical interpretation. The game is played by two players, ∀belard and ∃loise, who quarrel about the truth of a given formula. The player ∃loise, who argues in favour, plays when the formula is existential, say $\bigvee_i \phi_i$, by choosing an index $i_0$ ("∃loise's Choice"), after which the game is continued with the formula $\phi_{i_0}$. The player ∀belard, who argues against, plays when the formula is universal, say $\bigwedge_j \phi_j$, by choosing an index $j_0$, after which the game is continued with the formula $\phi_{j_0}$. The game ends when either ∀belard or ∃loise chooses the formula 0 or 1. Evidently, the game always terminates. If either ∃loise or ∀belard chooses 1, then ∃loise wins the game and ∀belard looses. Dually, if either ∃loise or ∀belard chooses 0, then ∀belard wins the game and ∃loise looses.

We have the following completeness result: the player ∃loise has a winning strategy for the game associated to the existential formula $\phi$ if and only if this formula $\phi$ is intuitionistically valid. (Every formula is equivalent to an existential formula by prefixing it with a singleton disjunction.)

For instance, there is no winning strategy for the formula

$$\bigwedge_k \bigvee_{n \geq k} \bigwedge_{m \geq k} f(n) \leq f(m),$$

because it is not possible to compute effectively such a minimum value for a function $f$.

The notion of classical validity, as described by Novikoff [Novikoff43], is inductively defined by the clauses

- 1 is valid,
- $\bigvee_i \phi_i$ is valid iff there exists $i_0$ such that $\phi_{i_0}$ is 1, or is an universal formula $\bigwedge_j \phi_{i_0 j}$ such that, for all $j$, the formula $\phi_{i_0 j} \vee \bigvee_i \phi_i$ is valid,
- $\bigwedge_i \phi_i$ is valid iff $\phi_i$ is valid for all $i$.

This definition may seem not well-founded, but it correctly defines classical validity as the smallest set satisfying the above closure properties.

For instance, a formula of the form $\psi \vee \bigvee_i \phi_i \vee \overline{\phi_{i_0}}$ is always valid. This is shown by induction on the formula $\bigvee_i \phi_i$. Firstly, recall that $\overline{\phi}$ is the usual defined complement of $\phi$, changing $\bigvee$'s into $\bigwedge$'s, 1's in 0's, and conversely. Second, $\phi_{i_0}$ is either 0 or 1, or a universal formula $\bigwedge_j \phi_{i_0 j}$ by the alternation of $\bigvee$'s and $\bigwedge$'s. In the first two cases, it is trivial to choose the index of a valid disjunct in the formula above. In the third case, choose the index such that we get the formula $\psi \vee \bigvee_i \phi_i \vee \overline{\phi_{i_0}} \vee \phi_{i_0 j}$, which is valid for all $j$ by the induction hypothesis.

The game semantics has to be adapted to the classical notion of validity: in the case of a disjunction $\bigvee_i \phi_i$, the game proceeds with the formula $\bigwedge_j [\phi_{i_0 j} \vee \bigvee_i \phi_i]$. The other cases do not change. A tentative interpretation of this definition is that it describes exactly a winning strategy for a game between ∀belard and ∃loise. This strategy is suggested by the inductive definition of classical validity: in the case of an existential formula, and after a choice $j_0$ of ∀belard, ∃loise should try again and choose a new $i$ in

$$\phi_{i_0 j_0} \vee \bigvee_i \phi_i,$$

using information drawn from $\phi_{i_0 j_0}$ (if this latter formula is 1, then ∃loise should choose this formula, of course).

There is such a winning strategy for the formula

$$\bigwedge_k \bigvee_{n \geq k} \bigwedge_{m \geq k} \phi_{nm},$$

with $\phi_{nm} = f(n) \leq f(m)$, which can be described as follows. The game starts by ∀belard giving a value $k$. The player ∃loise answers choosing an arbitrary value $n \geq k$, say $n = k$ and ∀belard answers by playing $m = m_0 \geq k$. The formula becomes

$$\phi_{k m_0} \vee \bigvee_{n \geq k} \bigwedge_{m \geq k} \phi_{nm}.$$

If $\phi_{k m_0}$ is true, then ∃loise wins. If $\phi_{k m_0}$ is false, the strategy for ∃loise is to choose the last value given by ∀belard. After ∀belard chooses a value $m = m_1 \geq k$, the formula becomes

$$\phi_{k m_0} \vee \phi_{m_0 m_1} \vee \bigvee_{n \geq k} \bigwedge_{m \geq k} \phi_{nm}.$$

The player ∃loise wins if $f(m_0) \leq f(m_1)$. In this way, to each game corresponds a sequence $m_0, m_1, \ldots$ such that $\phi_{km_0}$, $\phi_{m_0m_1}$, $\ldots$ are all false, i.e. such that $f(m_0) > f(m_1) > \ldots$ Since $\mathsf{N}$ is well-founded, ∃loise will win eventually by following this strategy.

## 2.4 Sequent Calculus versus Negative Translation

Both the negative translation and sequent calculus present a constructive explanation of some parts of mathematics that use the law of excluded middle.

It is instructive to compare both explanations in some concrete examples. On the 0/1 example, the sequent calculus seems much more suggestive than the negative translation, especially if we use the game-theoretic intuition.

## 2.5 Exercises on Part II

1. Do extraction of witnesses using sequent calculus, and compare with the Friedman's method. For instance, apply the sequent calculus to the exercises 9 and 10 of part I.

2. A concrete example of non-effective argument analysed by H. Schwitzenberg and U. Berger is the following proof for the existence of a greatest common divisor of two numbers $a$ and $b$, with $b > 0$ : the ideal $(a, b)$ generated by $a$ and $b$, contains an element $b > 0$, hence it contain a least element $c > 0$. Then $c$ is the greatest common divisor of $a$ and $b$. Apply the method of "trial and error" to guess what would be the computational content of this proof. (Hint: there are two parts in the proof, the first is the existence of a least element $c > 0$, the second that this least element $c$ divides both $a$ and $b$. The second part is effective. The first part is not: the interpretation is an algorithm that starts by claiming $c = b$, and whenever it is given an element $x \in (a, b)$ such that $0 < x < c$, "changes its mind" and take $c = x$ instead.)

## 2.6 References

[Aczel78] P. Aczel "An introduction to inductive definitions." In Hanbook of mathematical logic, J. Barwise ed., North-Holland, p. 739-782.

Presents the notion of inductive definitions in a simple and clear way.

[Buchholz] W. Buchholz, S. Feferman, W. Pohlers and W. Sieg *Iterated Inductive Definitions and Subsystems of Analysis.* LNM 897.

One quite important point is that the negative translation does not work in presence of generalised inductive definitions. (In the next section, we will see that it does not work in presence of the Axiom of Choice.) If one thinks of generalised inductive definitions as least prefixed point of *strictly* positive operators (see [Aczel78]), one needs least prefixed point of positive operators, not necessarily strictly positive.

One main theme of this book is to present various methods that explain effectively the combination of generalised inductive definitions and classical logic. Three such methods are presented, and two of them are based on sequent calculus. Interestingly, cut-elimination is not proved in general, but only for sequents that have only positive occurence of the inductively defined predicate.

[Bernays] "On the original Gentzen consistency proof for number theory" in Intuitionism and Proof Theory, Kino, Myhill, Vesley eds, pp. 409-417

[Gentzen69] G. Gentzen *Collected Works.* M.E. Szabo ed., North-Holland.

The reading of the original paper of Gentzen, especially the beginning of his first paper on consistency proof for classical arithmetic, and the presentation by Bernays are quite instructive. In particular, the paper of Gentzen contains a remarkable formal analysis of Euclid's proof of the infinity of prime numbers. In both papers there appears clearly the characteristic "multi-conclusion" feature of classical logic, which seems to indicate that a classical proof of an existential statement may contain potentially several witnesses, in opposition to a constructive proof.

[Tait68] W. W. Tait "Normal Derivability in Classical Logic." Springer Lecture Notes in Mathematics 72, J. Barwise ed, pp. 204-236.

The presentation is elegant and the goals and methods clearly stated. Let us cite a part of the introduction. "Also we will be dealing with infinitary propositions and infinite derivations of them, we will deal with these constructively—not, of course, in the narrow sense of Hilbert's finitism, but in the wider sense which admits (potential) infinities, in the form of rules of construction, as objects. As a consequence of this, we will obtain a constructive foundation for infinitary classical logic and for those parts of mathematics contained in it." It is to be noticed that Tait's paper had a deep influence on further proof-theoretic analysis of subsystems of second-order arithmetic, as can be seen in the survey on inductive definitions [Buchholz].

[ML68] P. Martin-Löf *Notes on Constructive Mathematics.* Almqvist & Wiksell ed.

Another elegant presentation of sequent calculus is contained in the monograph of Martin-Löf. It presents a constructive explanation of the notion of Borel sets for Cantor space, using a sequent calculus where formulae are Borel sets. In this work there also appears clearly the fact that cut-elimination can be formulated as the *admissibility* of the cut rule in a system that presents inductively the cut-free provability of a sequent. This can be traced back to the first proof of Gentzen, and to Lorenzen, who introduced the notion of admissibility of a rule while analysing Gentzen's work.

[Novikov43] P.S. Novikoff "On the consistency of certain logical calculus." Matematiceskij sbornik (Recueil Mathématique) T. 12 (54), pp. 230-260.

[Coquand95] Th. Coquand "A Semantics of Evidence of Classical Arithmetic." Journal of Symbolic Logic 60 (1995), pp. 325–337.

Contains an analysis of cut-elimination based on a game-theoretic interpretation of proofs. Cut-elimination is seen as an interaction between two strategies, and the termination of cut-elimination is proved by an analysis of the structure of this interaction.

# 3 Axiom of Choice and Hilbert's Program

It is known that the Axiom of Choice is constructively valid, and this fact has been emphasized by Martin-Löf [Martin-Lof73]. As discussed in Bishop's book on constructive analysis, the well-known problems or "paradoxical consequences" of the Axiom of Choice in non-constructive mathematics, like the non-effective "existence" of a well-ordering of the reals or the Banach-Tarski paradox, use in an essential way a combination of this axiom with the law of excluded middle.

In the first part, we analyse in detail a logical problem that arises from this combination. We can thus formulate one of the open problems in proof-theory connected to this part: is it always possible to transform a proof of an existential statement that uses classical logic and the axiom of choice into a constructive proof of the same statement? This chapter is in part extracted from the paper [Berardi95].

We end with a short presentation of Hilbert's program.

## 3.1 Presentation of $\mathsf{HA}^\omega$

In order to formulate precisely what is the problem with the combination of the Axiom of Choice and the Law of Excluded Middle, we describe a formal system $\mathsf{HA}^\omega$ that allows quantification over functions (but in a quite "weak" way, since it is conservative over $\mathsf{HA}$ even extended with the Axiom of Choice, this is Goodman's result.)

### 3.1.1 Types

The types of $\mathsf{HA}^\omega$ are $\mathsf{N}$ and with $\tau, \tau'$ also $\tau \to \tau'$. Here and below types will be denoted by lower case Greek letters $\tau, \tau', \ldots$.

### 3.1.2 Terms

The terms of $\mathsf{HA}^\omega$ are built from (typed) variables and constants using lambda abstraction and (well typed) application. There are countably many variables $x, y, z, \ldots$ for each type $\tau$. The constants are: $\mathsf{0} : \mathsf{N}$, $\mathsf{s} : \mathsf{N} \to \mathsf{N}$ and finally $\mathsf{R}_\tau : \tau \to (\mathsf{N} \to \tau \to \tau) \to \mathsf{N} \to \tau$ for every type $\tau$. Terms are denoted by $M, M', N, \ldots$, and $M : \tau$ expresses that the term $M$ has type $\tau$.

### 3.1.3 Formulae

Prime formulae are equations of the form $M = M'$, with $M, M' : \mathsf{N}$. Higher type equations, say $M = M'$ with $M, M' : \mathsf{N} \to \mathsf{N}$, are abbreviations of equations of lowest type, such as $Mx = M'x$ with $x$ fresh. The set of formulae of $\mathsf{HA}^\omega$ is generated in the usual way from the prime formulae by the boolean connectives $\wedge, \Rightarrow, \perp$ and the quantifiers $\forall, \exists$. We use $\phi, \phi', \ldots$ to denote formulae. We abbreviate $\phi \Rightarrow \perp$ by $\neg\phi$.

### 3.1.4 Theory

The theory $\mathsf{HA}^\omega$, intuitionistic higher-order arithmetic, is built up from three parts: (i) axioms and rules for first order many-sorted intuitionistic predicate logic; (ii) equality axioms and the axiom schema of induction; (iii) lambda calculus axioms and rules and the defining equations of the constants $\mathsf{R}_\tau$, which are: $\mathsf{R}_\tau xy\mathsf{0} = x$, $\mathsf{R}_\tau xy(\mathsf{s}z) = yz(\mathsf{R}_\tau xyz)$. Thus our theory $\mathsf{HA}^\omega$ essentially coincides with $\mathsf{HA}^\omega$ from [Troelstra344], the only difference being that we consider $\vee$ as defined and use the lambda version instead of the combinator version. The theory $\mathsf{HA}^\omega_c$ is $\mathsf{HA}^\omega$ with classical logic; $\mathsf{HA}^\omega_-$, minimal higher-order arithmetic, is $\mathsf{HA}^\omega$ without the axiom schema $\bot \Rightarrow \phi$.

### 3.1.5 The Axiom of Choice

Theories of classical (intuitionistic) analysis can be obtained from $\mathsf{HA}^\omega_c$ ($\mathsf{HA}^\omega$) by adding the axiom of choice. The axiom of choice of types $\tau, \tau'$, denoted by $\mathsf{AC}(\tau, \tau')$, is the axiom schema

$$[\forall x : \tau\ \exists y : \tau'\ \phi(x, y)] \Rightarrow \exists f : \tau \to \tau'\ \forall x : \tau\ \phi(x, fx)$$

(schematic in formula $\phi$). Here we will mainly consider $\mathsf{AC}(\mathsf{N}, \tau)$ (schematic in $\tau$), that we may abbreviate to $\mathsf{AC}$. The axiom $\mathsf{AC}$ is sufficiently strong to formalize a large part of classical analysis. Intuitionistically, $\mathsf{AC}$ is not a strong axiom, as may be expected from the Brouwer–Heyting–Kolmogorov interpretation of a $\forall\exists$ prefix. More formally, it follows from results of Goodman [Goodman70] that adding $\mathsf{AC}(\mathsf{N}, \mathsf{N})$ and $\mathsf{AC}(\mathsf{N}, \mathsf{N} \to \mathsf{N})$ to $\mathsf{HA}^\omega$ is conservative over Heyting Arithmetic.

### 3.1.6 A negative interpretation

We will use the notation $\nabla\ \phi$ for $\neg\neg\phi$. This notation is justified by the fact that $\neg\neg$ can be thought of as a modal operator on formulae; indeed we can prove that $\nabla\ \phi$ follows from $\phi$, and $\nabla\ \psi$ from $\nabla\ \phi$ and $\phi \Rightarrow \nabla\ \psi$.

Since absurdity is not interpreted by the empty type, we cannot realize $\bot \Rightarrow \phi$ for all $\phi$. We overcome this problem by exercising some care in the negative interpretation. The idea is due to Kolmogorov. We employ the fact that $\bot \Rightarrow \nabla\ \phi$ can be proved for all $\phi$ without using the axiom schema $\bot \Rightarrow \phi$. Although our prime formulae are decidable, the negative interpretation of a prime formula $\phi$ will be $\nabla\ \phi$.

As negative interpretation we use a standard version of the double negation translation, i.e. prefixing prime formulae and $\exists$ by $\nabla$. The negative interpretation of a formula $\phi$, denoted by $\mathsf{D}\phi$, is inductively defined by:

- $\mathsf{D}\bot \equiv \bot$
- $\mathsf{D}\phi \equiv \nabla\ \phi$ if $\phi$ is a prime formula
- $\mathsf{D}[\phi \Rightarrow \psi] \equiv [\mathsf{D}\phi] \Rightarrow \mathsf{D}\psi$

- $\mathsf{D}[\phi \wedge \psi] \equiv \mathsf{D}\phi \wedge \mathsf{D}\psi$
- $\mathsf{D}\forall x : \tau\ \phi \equiv \forall x : \tau\ \mathsf{D}\phi$
- $\mathsf{D}\exists x : \tau\ \phi \equiv \nabla\ \exists x : \tau\ \mathsf{D}\phi$

Here and below, $\equiv$ denotes syntactical identity.

The negative interpretation satisfies the following preservation property: if $\phi$ is provable in $\mathsf{HA}^\omega_c$, then $\mathsf{D}\phi$ is provable in $\mathsf{HA}^\omega_-$. In the presence of AC, one cannot expect such a simple preservation result since, as we shall see below, AC is much stronger classically than it is intuitionistically.

The theory $\mathsf{HA}^\omega_- + \mathsf{D}\ \mathsf{AC}$ will be called *negative analysis.* We need the following technical results.

**Lemma 1** *The following schemata are provable in* $\mathsf{HA}^\omega_-$*:*

*(i)* $\bot \Rightarrow \nabla\ \phi$*;*

*(ii)* $\neg\nabla\ \phi \iff \neg\phi$*;*

*(iii)* $\phi \Rightarrow \nabla\ \phi$*;*

*(iv)* $\mathsf{D}\phi \iff \nabla\ \mathsf{D}\phi$*,*

*(v)* $\mathsf{D}\exists x : \tau\ \phi \iff \nabla\ \exists x : \tau\ \phi$*, if* $\phi$ *is a prime formula;*

*(vi)* $\phi \Rightarrow \mathsf{D}\phi$*, if* $\phi$ *is a prenex formula not containing* $\Rightarrow$*;*

*(vii)* $\mathsf{D}\neg\phi \iff \neg\mathsf{D}\phi$*.*

**Proof:** The clauses (i)-(iii) and (vi),(vii) are trivial. For (iv), observe that the standard proof of this fact by formula induction does not use the axiom schema $\bot \Rightarrow \phi$. For all $\phi$ we have $\nabla\ \exists x : \tau\ \nabla\ \phi \iff \nabla\ \exists x : \tau\ \phi$ via $\neg\exists x : \tau\ \phi \iff \forall x : \tau\ \neg\phi$ using (ii), so we have (v).

The negative interpretation of AC, DAC, reads:

$$[\forall x : \mathsf{N}\ \nabla\ \exists y : \tau\ \mathsf{D}\phi(x, y)] \Rightarrow \nabla\ \exists f : \mathsf{N}{\rightarrow}\tau\ \forall x : \mathsf{N}\ \mathsf{D}\phi(x, fx).$$

By the stability[4] of formulae after the negative interpretation, which follows from Lemma 1.1 (iv), DAC is subsumed by the following axiom schema:

$$[\forall x : \mathsf{N}\ \nabla\ \exists y : \tau\ \neg\phi(x, y)] \Rightarrow \nabla\ \exists f : \mathsf{N}{\rightarrow}\tau\ \forall x : \mathsf{N}\ \neg\phi(x, fx)$$

*Par abus de langage* we will from now on denote this schema by DAC.

We can now extend the preservation property above to: if $\phi$ is provable in classical analysis, then $\mathsf{D}\phi$ is provable in negative analysis. The proof goes by inspection of the standard preservation proof, taking care that $\bot \Rightarrow \phi$ is avoided using the lemma above.

[4]A formula is stable iff it is equivalent to the negation of another formula.

## 3.2 Classical Logic and the Axiom of Choice

In this section, we enumerate some known difficulties in giving a constructive interpretation of the Axiom of Choice in the presence of classical logic. The main remark is that DAC fails to be an intuitionistic consequence of the Axiom of Choice[5]. We point out three independent reasons:

- DAC makes problematic the constructive interpretation of the notion of function; actually, it refutes Church's Thesis;
- DAC is proof theoretically very strong, we can actually interpret by DAC impredicative second-order comprehension, so that one cannot give any predicative interpretation of DAC;
- a standard computational interpretation of classical arithmetic, the one using infinitary propositional calculus, that we presented in part II, when extended to quantification over functions, fails to interpret the Axiom of Choice.

### 3.2.1 DAC refutes Church's Thesis

In the classical system $\mathsf{HA}^\omega_c + \mathsf{AC}$, we may define the characteristic function of any predicate. Indeed, for any statement $\phi(x)$, we have

$$\exists f\ \forall x\ [\phi(x) \iff [f(x) = 0]]$$

since, by the Excluded Middle,

$$\forall x\ \exists y\ [\phi(x) \iff [y = 0]].$$

If we take for $\phi$ some non-decidable formula, then we may prove in this way the existence of non-recursive functions in $\mathsf{HA}^\omega_c + \mathsf{AC}$.

In other words, we refute in $\mathsf{HA}^\omega_c + \mathsf{AC}$ the formula

$$\mathsf{CT} \equiv \forall f : \mathsf{N}{\to}\mathsf{N}\ \exists e : \mathsf{N}\ \forall x : \mathsf{N}\ \exists y : \mathsf{N}\ [T(e, x, y) \wedge U(y) = f(x)]$$

where $T(e, x, y)$ is the standard Kleene predicate (which can be formulated as an equation) and $U(y) = z$ means that the output of the computation with code $y$ is $z$. This formula CT expresses Church's Thesis in an intuitionistic way, stating that every function $f$ has a recursive code $e$.

This simple remark has some deep consequences. Since CT is a prenex formula, it implies its negative translation DCT by lemma 1.1 (vi). We can thus prove $\perp$ in the system $\mathsf{HA}^\omega_{-} + \mathsf{DAC} + \mathsf{CT}$. In other words, if we assume D AC, we can prove in $\mathsf{HA}^\omega_{-}$ that not all functions are recursive (even if we cannot exhibit a counterexample!).

A direct corollary is that there cannot be any recursive realization of D AC. For exactly this reason, and because the semantics of the system NuPrl is based on

[5]This is to be contrasted with the induction schema over integers, whose negative interpretation is an instance of the induction schema.

recursive realizability, the work [Mur90] restricts itself to a fragment of classical logic that does not include the Axiom of Choice. This often forces one to encode functions as relations, and this encoding may be unnatural (see the discussion of Higman's lemma in [Mur90]).

### 3.2.2 Proof Theoretic Strength of D AC

A second difficulty in interpreting D AC comes from the fact that in intuitionistic logic, D AC is proof-theoretically much stronger than AC.

We have seen already that $\mathsf{HA}^\omega + \mathsf{AC}$ is conservative over HA [Goodman]. In contrast, by using the fact that in $\mathsf{HA}^\omega_c + \mathsf{AC}$ we may define the characteristic function of any predicate, it is not difficult to see that we can interpret the second-order comprehension axiom in $\mathsf{HA}^\omega_= + \mathsf{D\ AC}$. This system is proof theoretically much stronger than HA (see, for instance, Shoenfield's book on Mathematical Logic, Section 8.5), which implies that there cannot be any predicative way of modeling $\mathsf{HA}^\omega_= + \mathsf{D\ AC}$.

These remarks may explain a comment of Gödel after presenting the negative interpretation (see his Collected Work): "Intuitionism appears to introduce genuine restrictions only for analysis and set theory; these restrictions, however, are due to the rejection, not of the principle of Excluded Middle, but of notions introduced by impredicative definitions."

An important aspect that is not covered in this comment however is a more "intensional" aspect of logical systems, independently of their proof-theoretic strength. From an intuitionistic viewpoint, the proof object, that counts as evidence for the truth of a proposition, is of primary importance.

### 3.2.3 Problem in sequent calculus

Let us analyse now another way to get a possible computational content from classical arguments by considering Gentzen's sequent calculus formulation of classical arithmetic. One elegant approach is to use derivations in infinitary propositional logic. There is a general cut-elimination result for this logic which gives a computational interpretation of proofs. If we introduce countable disjunction and conjunction, we can interpret in this way classical quantification over natural numbers and give a computational interpretation of proofs in classical arithmetic.

A natural attempt is then to introduce disjunction and conjunction over the set of all number theoretic functions, and hope that we can interpret in this way classical quantification over number theoretic functions. However, as noticed in Tait's paper (see the reference in part II), there is a natural formulation of the Axiom of Choice in infinitary propositional logic. We start from atoms $\phi_{mn}$, $\overline{\phi_{mn}}$, and axioms

$$\Gamma, \phi_{mn}, \overline{\phi_{mn}}$$

and we ask whether it is possible to build a cut-free proof of

$$\bigvee_m \bigwedge_n \overline{\phi_{mn}}, \bigvee_f \bigwedge_m \phi_{mf(m)}, \tag{3.1}$$

from these axioms. It is not difficult to see that there cannot be such a cut-free proof. We will explain this in some detail.[6] Assume by contradiction $\Delta$ is a cut-free proof of (3.1).

First, observe that all conjunctions in (3.1) are countable, so by the subformula property all conjunctions in $\Delta$ are countable, so that $\Delta$ is at most countably branching. Since $\Delta$ is also well-founded, it follows that $\Delta$ is countable and that at most countably many functions $f_0, f_1, \ldots$ appear in $\Delta$.

Second, replace every subformula of the form $\bigvee_f \ \phi(f)$ in $\Delta$ by $\bigvee_k \ \phi(f_k)$ and call the resulting tree $\Delta'$. Observe that $\bigvee_f \ \phi(f)$ can only be introduced in $\Delta$ from some $\phi(f_k)$. It follows that $\Delta'$ is indeed a proof of

$$\bigvee_m \bigwedge_n \overline{\phi_{mn}}, \ \bigvee_k \bigwedge_m \phi_{mf_k(m)}.$$

Third, the above conclusion of $\Delta'$ is false. This can be seen by taking $f$ to be a function diagonalizing over $f_0, f_1, \ldots$, e.g. $f(n) = f_n(n) + 1$, and $\phi_{mn} \iff f(m) = n$. Indeed, $\bigvee_m \bigwedge_n \overline{\phi_{mn}}$ is false since $f$ is total, and $\bigvee_k \bigwedge_m \phi_{mf_k(m)}$ is false since $f$ is by construction different from all $f_k$'s.

## 3.3 Hilbert's Program

At the core of Hilbert's program [Hilbert], was the problem of making constructive sense of classical reasoning that uses the axiom of choice.

We recall here the idea of Hilbert for attacking this problem, idea that we shall reformulate in the next chapter in a constructive framework. The idea is to look at the axiom of choice in the form of an operator $\epsilon$ that is like an oracle that "chooses" an element. Typically, we introduce a functional $\epsilon(f)$ on functions such that

$$f(x) = 0 \Rightarrow f(\epsilon(f)) = 0.$$

The immediate problem is that we cannot describe effectively such a functional. This is clear by a continuity argument: were $\epsilon$ computable, only a finite number of values of $f$ would be used in the computation of $\epsilon(f)$. If $f_0$ is the constant function 1, and $n_0 = \epsilon(f_0)$, we get a contradiction by considering the function $g$ which is 1 only on $n_0$ and the values of $f$ needed in the computation of $\epsilon(f_0)$, and 0 otherwise. We should have indeed $\epsilon(g) = \epsilon(f_0) = n_0$, but $g(n_0) = 1$ and there exists $n$ such that $g(n) = 0$.

In order to solve this difficulty, Hilbert suggested looking at the operator $\epsilon$ as an "ideal" object, not having a "real" existence. Its purpose is only to simplify the theory, like the introduction of complex numbers in the theory of equations, or the introduction of ideal points at infinity in projective geometry. A main difference however is that complex numbers can be given a meaning as a pair of reals. Here, if it is not possible to explain what is this "ideal" object $\epsilon$ in general, to give a constructive model of it, Hilbert thought it would be possible to explain

[6] Cf. Tait's paper. Tait describes this result as known already, but does not give further references. We think he was thinking to a proof using boolean models, as presented in the appendix.

its meaning *in any given proof* of a concrete statement. The reason is intuitive: in any given proof, we can only have used a finite amount of information about this "ideal", "infinitary" object, and hence we should be able to replace it by a finite approximation. Notice that we did already meet this restriction to proofs of "finitary result" in Friedman's method. This method transforms non-effective proofs of a statement into an effective proof of the same statement only if this statement is purely existential.

What is important to notice here is that this interpretation by a finite approximation is relative to a given proof of a concrete statement. This is to be contrasted with the usual semantics, where the interpretation does depend only of the statement, and not of its proof.

Hilbert introduced a stratification of different uses of the axiom of choice in classical mathematics:

1. at the first level, we have the axiom of choice over natural numbers $AC(o, o)$,
2. the next level is the axiom of choice over functions $AC(o{\rightarrow}o, o)$,
3. the third level, used for proving for instance the existence of a well-ordering of the reals, requires the extensional form of $AC(o{\rightarrow}o, o)$.

The first level contains the problem of explaining constructively second order arithmetic. This is still an open problem. However, it is remarkable that in some mathematically interesting examples, it is possible to explain constructively the use of the Axiom of Choice by the technique of formal or point-free, topology.

## 3.4 Exercises on Part III

1. Show that it is not possible to give a negative translation for Martin-Löf's Intuitionistic Type Theory. (Hint: with the use of $\Sigma$ types, it is possible to interpret the Axiom of Choice in Type Theory with one universe, while in Beeson's book for instance, it is shown that Type Theory with one universe is proof theoretically weaker than second order arithmetic.)

## 3.5 References

[Troelstra344] A. Troelstra "Metamathematical investigation of intuitionistic arithmetic and analysis" LNM 344.

[Beeson85] M. Beeson *Foundations of Constructive Mathematics.* Berlin, Springer-Verlag.

Contains interesting historical discussions, and a proof of Goodman's result that $\mathsf{HA}^\omega + \mathsf{AC}$ is conservative over $\mathsf{HA}$.

[Mur90] Ch. Murthy "Extracting Computational Content from Classical Proofs." Ph. D. Thesis, Cornell.

The analysis of the non-effective proof of Higman's lemma explains clearly on a concrete mathematical example the problem of combining Excluded Middle with the Axiom of Choice.

[Martin-Lof73] P. Martin-Löf "An Intuitionistic Theory of Types: predicative part." Logic Colloquium 73, North-Holland, 1975, p. 73-118.

Presents a derivation of the Axiom of Choice in Type Theory, and emphasizes the intuitionistic validity of the Axiom of Choice.

[Goodman] N. Goodman. *Intuitionistic arithmetic as a theory of constructions.* PhD thesis, Stanford University, 1968. There are more accessible references in JSL 37, p. 225-246 and in LNM 337.

Contains a proof that the Axiom of Choice added to $\mathsf{HA}^\omega$ still leads to a theory conservative over $\mathsf{HA}$. This is to be contrasted with the situation in classical logic, where the addition of the Axiom of Choice is not well understood yet.

[Hilbert] D. Hilbert "Die logischen Grundlagen der Mathematik." Math. Annalen 88 p. 151-65, 1923

"Ueber das Unendliche." Math. Annalen 95, 1926.

"Probleme der Grundlagen der Mathematik." Math. Annalen 102, 1929.

[Tait68] W. W. Tait "Normal Derivability in Classical Logic." Springer Lecture Notes in Mathematics 72, J. Barwise ed, pp. 204-236.

[Berardi95] S. Berardi, M. Bezem, Th. Coquand "On the computational content of the Axiom of Choice." In proceeding of TLCA 95, LNCS 902.

Contains a rather direct computational interpretation of the negative translation of the axiom of choice. The normalisation property is proved using excluded middle and dependent choices. The algorithmic structure of the interpretation of some proofs (like Higman's lemma) seems however interesting.

There is a theorem in topos theory (Barr's theorem) that claims that if a geometric statement is proved from a geometric theory using classical logic and axiom of choice, then it can be proved intuitionistically. However, the proof of this statement uses the axiom of choice and classical logic.

# 4 Formal Topology

The Axiom of Choice is often used, combined with the Law of Excluded Middle, in the form of Zorn's lemma to prove the existence of objects such as prime ideals, maximal ideals, Henkin sets, ultrafilters ... We have seen in the previous section that both negative translation and sequent calculus fail to explain constructively such use of the Axiom of Choice.

While it is still an open problem to have a general explanation, we present in this chapter a method that explains effectively some uses of Zorn's lemma. This method is best seen as a combination of two notions: the notion of *topological models*, where truth-values become open of suitable topological spaces, and the notion of *formal spaces*, by which we can describe in an effective way these models.

## 4.1 Historical Roots

The idea of point-free topology seems to go back to Whitehead (around 1910), and it was first presented by Russell (see [Russell14]). The 1935 paper by Moore [Moore35] presents a point-free version of the plane and the sphere, while Menger [Menger] presents a survey of some notions of point-free topology in 1940. The main application for Russell was an analysis of the use of mathematical abstractions in representing the physical world. The idea was to define the objects of mathematical physics as functions of observable sense-data, thus explaining abstract mathematical objects in term of concrete things. This is a kind of converse of the usual view, that explains sense-data as functions of physical objects. The advantage of this change of point of view is to make the application of mathematics to physics somewhat less mysterious.

This is the core of the idea of point-free/formal topology: to explain an ideal, infinitary object like a point in terms of concrete finitary objects.

For instance, in some papers by Wiener [Wiener14], the notion of instant of time is analysed in terms of event.

One major problem that Russell mentions is the need to use the Axiom of Choice, for building points. Russell formulated the problem as follows: "It is shown that the existence of instants require hypotheses which there is no reason to suppose true - a fact which may be not without importance in physics." One of the hypotheses here was that "the whole class of events can be well ordered" [Russell36].

## 4.2 Formal Topology

### 4.2.1 Locales

The idea of point-free topology has been revived recently in the framework of locales [Stone] and, in computer science, with the notion of information systems [ML83,Scott82,Vickers89]. The problem of using the Axiom of Choice in the construction of points gets in this framework a subtle partial solution, that is described by Johnstone [1981]. In term of the theory of locales, it is noticed that "the category of locales is actually more convenient in many ways than the category of spaces" and that we can develop a constructive theory of spaces by staying at the level of the presentation of the spaces, without ever mentioning the points. Johnstone credits to Isbell the idea that the category of locales may have even better properties than the usual category of topological spaces.

### 4.2.2 Relevance to the analysis of the Axiom of Choice

In what way is the problem raised by Russell of the use of constructing points solved partially by the theory of locales?

This is best understood by looking at some examples of Stone's duality between the algebraic structure of boolean algebra and topological structure of totally disconnected compact spaces [Stone]. Any element of a boolean algebra can be seen as defininig a closed open subset of the associated space, which, as a set, is the set of all ultrafilters of the boolean algebra. This duality gives a kind of dictionary between topological notions (infinitary) and algebraic notions (finitary). For instance: the notion of space correspond to the notion of algebra, continuous maps corresponds to algebraic morphisms, open subsets correspond to ideals.

A typical example is Cantor space $\mathsf{C} = \{0,1\}^{\mathsf{N}}$. As a formal space, this is nothing but the boolean algebra built freely on a countable number of atoms.

An open subset of the space corresponds to an ideal of this boolean algebra seen as a ring. Namely, if $U$ is an open subset, the set of closed open subsets included in $U$ forms an ideal, and conversely we can associate to an ideal the open union of its elements thought of as closed open susbets. If we have a family of ideals $I_k$, the union of these ideals seen as an open of the space corresponds to the ideal $\Sigma I_k$ which is the ideal of elements that can be written $x_{k_1} + \ldots + x_{k_p}$ for a finite family $x_{k_j} \in I_{k_j}$.

The fact that we can extract a finite covering from any covering becomes in this way the fact that if 1 belongs to an ideal $\Sigma I_k$ where $(I_k)$ is a family of ideals, then we can find $k_1, \ldots, k_p$ such that 1 belongs to $I_{k_1} + \ldots + I_{k_p}$. This is direct because if $1 \in \Sigma I_k$ we can by definition write $1 = x_{k_1} + \ldots + x_{k_p}$ for some $x_{k_j} \in I_{k_j}$ and hence 1 is already in some finite sum $I_{k_1} + \ldots + I_{k_p}$.

We see that the compactness of Cantor space is direct and constructive if expressed in a point-free way. This can be contrasted with the usual form of compactness whose proof is some form of König's lemma[7]. From a classical point of view, the use of the Axiom of Choice has been "factorised" in the proof of the duality theorem between spaces and algebras.

It is sometimes surprising how usual topological notions correspond in this way to usual algebraic notions. As we have seen, an open $U$ corresponds to an ideal $I$ (the ideal of closed open subsets that are subset of $U$). To say that $U$ is everywhere dense is equivalent to $I^{\perp} = 0$, that is $x = 0$ whenever $xy = 0$ for all $y \in I$.

Sometimes however, an (apparently!) simple topological notion corresponds to a more subtle algebraic construction. For instance, if $X_1, X_2$ are respectively the

[7]More generally, one can define the product of spaces in a point-free way, and prove Tychonoff's theorem directly [Stone]. The classical version of this theorem is equivalent to the Axiom of Choice.

spaces corresponding to the algebras $B_1$ and $B_2$, the product $X_1 \times X_2$ corresponds to a kind of tensor product $B_1 \otimes B_2$ whose direct algebraic description is subtle (it is *not* the algebraic product of $B_1$ and $B_2$ which corresponds to the sum of $X_1$ and $X_2$). In the other direction, we can give as example the Baire theorem, which corresponds to a simple lemma known as Tarski's lemma [Feferman].

What is striking from a proof theoretic viewpoint is that infinitary notions on one side are replaced by finitary notions on the other side. Often not only the use of the Axiom of Choice, but also of the law of excluded middle disappear on the algebraic side [Stone].

Formal topology generalises this to more general kind of topological spaces.

### 4.2.3 Formal Spaces

We now present one possible definition of formal spaces in a predicative framework. The importance of this restriction is that we want to analyse some impredicative proofs using the theory of locales in a predicative way. The definition we present is due to Sambin [Sambin87].

A formal space is a commutative monoid $S$ with unit, together with a covering relation $x \lhd U$ between elements of $S$ and subsets of $S$ satisfying the following conditions.

- if $x \in U$, then $x \lhd U$,
- if $x \lhd U$, and $U \lhd V$ then $x \lhd V$, where $U \lhd V$ means that $u \lhd V$ for all $u \in U$,
- if $x \lhd U$ and $x \lhd V$, then $x \lhd UV$, where $UV$ is the set of all elements $uv$ for $u \in U,\ v \in V$,
- if $x \lhd U$ then $xy \lhd U$.

Intuitively the elements of $S$ represents basic opens, the monoid operation the intersection of basic opens, and $x \lhd U$ means that the basic open $x$, as a set of points, is contained in the union of all basic open in $U$. A formal open in general is a subset of $S$, thought of as the union of its elements.

A *formal point* of a space $(S, 1, ., \lhd)$ is a predicate $\alpha$ on the set $S$ such that[8]

- $\alpha(1)$,
- if $\alpha(x.y)$ then $\alpha(x)$,
- if $x \lhd U$, and $\alpha(x)$ then there exists $y \in U$ such that $\alpha(y)$,
- if $\alpha(x)$ and $\alpha(y)$ then $\alpha(x.y)$.

For instance, any boolean algebra $B$ defines in a canonical way a formal space. We define $x \lhd U$ as meaning that $x$ belongs to the ideal generated by $U$. We can then check that all four properties above are satisfied.

[8] We can see in the examples below the importance of a distinction between the "kind" of objects considered here: basic open are to be thought of as "concrete objects" while open in general are predicates. The points of a space also are predicates. These fundamental distinctions may be lost in a presentation of formal topology which uses freely impredicativity.

#### 4.2.4 Phase Semantics

We will use often the following construction of formal spaces. Let $S$ be a commutative monoid, and $Z \subseteq S$ a subset of $S$. For $U \subseteq S$, we define $U^\perp$ as $\{x \in S \mid xU \subseteq Z\}$ where $xU$ is the set $\{xu \mid u \in U\}$. If $x \in S$ we write $x^\perp$ for $\{x\}^\perp$.

**Proposition:** If $Z \subseteq S$ is such that

- if $x \in Z,\ y \in S$ then $xy \in Z$,
- if $x^2 \in Z$, then $x \in Z$,

then the relation $x \lhd U$ defined by $U^\perp \subseteq x^\perp$ defines a covering on $S$.

This proposition has a direct proof. Notice that $U \lhd V$ iff $V^\perp \subseteq U^\perp$. It can be noticed that the complete Heyting algebra of saturated subsets, such that $U = U^{\perp\perp}$ is actually a complete *boolean* algebra. We refer to [Sambin] for an analysis of the notion of complete Heyting algebra in a predicative metalanguage like Intuitionistic Type Theory[9].

This space is called the *space of phases* defined by $S$ and $Z$.

### 4.3 Topological models

The idea of seeing an open of an ordinary topological space as a generalized truth value goes back at least to Stone and Tarski.[10]

This is possible in general only if the logic is intuitionistic. The negation of an open $U$ is interpreted as the interior of its complement, while its double negation is the interior of its closure, which does not coincide with $U$ in general. Excluded middle is thus not validated by topological models in general.

This interpretation generalizes directly if we use formal spaces. The method we use can then be described as follows.

We start from a set of conditions[11]. Often this set cannot be satisfied in a effective way, and we need Zorn's lemma realize them. What we do instead is to realize *effectively* these conditions in a "relativized sense", where the conditions are interpreted as open of a suitable formal space $Y$[12].

Of course, we have realised these conditions only in a "weak" sense. However, the next sections show that, if the formal space $Y$ is non trivial, this "weak" realization may be enough for some applications.

---

[9]The key point is a distinction between *sets* (small collections) and *types* (large collections). The support of a complete lattice will be in general a *type* and what is required is the existence of a least upper bound for any *set*-indexed family of elements.

[10]They consider only propositional logic; this was generalised later to first-order logic by Mostowski [Mostowski]. It should be noted the early paper by Tsao-Chen [Tsao] pointing out very clearly the connection between topology and modal logic.

[11]This set of conditions has to be expressed as a so-called geometric theory.

[12]It is important to remark that we can present effectively these models, and indeed, following [Sambin], this presentation can be done in Intuitionistic Type Theory.

## 4.4 Prime Filters

A simple example of this "elimination of the use of the Axiom of Choice" is the existence of prime ideals for a distributive lattice. Given such a lattice $\mathsf{D}$, we consider the elements of $\mathsf{D}$ as basic opens, and we define a covering relation $x \lhd U$, for $U$ subset of $\mathsf{D}$, by "there exists $x_1, \ldots, x_k \in U$ such that $x \leq x_1 \vee \ldots \vee x_k$." In particular, if $1 \lhd \emptyset$ then $1 \leq 0$ and the lattice has only one point. Notice also that $x \lhd y$ holds iff $x \leq y$.

What would be a point of this space? We can see it as a predicate $\mu(x)$ on $\mathsf{D}$ such that:

- $\mu(1)$,
- $\neg\mu(0)$,
- $\mu(x), \mu(y) \rightarrow \mu(x \wedge y)$,
- $\mu(x \vee y) \rightarrow [\mu(x) \vee \mu(y)]$.

Thus a point of this space is exactly a prime filter of the distributive lattice $\mathsf{D}$.

If we don't have the last condition, we can find explicitely such a predicate $\mu$ by taking $\mu(x)$ to be $z \leq x$ where $z$ is an element such that $\neg[z \leq 0]$ holds. But, in general, it is *not* possible to describe effectively a predicate $\mu$ satisfying these conditions together with $\mu(x \vee y) \rightarrow [\mu(x) \vee \mu(y)]$.

If we interpret $\mu(x)$ as the basic open $x$ of the space defined by $\lhd$[13], we do realise *effectively* all these conditions. For instance, the condition

$$\mu(x) \rightarrow [\mu(y) \rightarrow \mu(x \wedge y)]$$

is satisfied, because if $z \lhd x$ and $z \lhd y$ then $z \leq x$, $z \leq y$ and hence $z \leq x \wedge y$ and $z \lhd x \wedge y$. The last condiction holds because $x \vee y$ is covered by $\{x, y\}$.

## 4.5 Prime Ideals

Let $A$ be a commutative ring with unit. We list conditions on a predicate $\nu$, such that $\nu(x)$ would say classically that $x$ is *not* in a fixed prime ideal.

1. $\nu(1)$,
2. $\neg\nu(0)$,
3. $\nu(x), \nu(y) \rightarrow \nu(xy)$,
4. $\nu(xy) \rightarrow \nu(x)$,
5. $\nu(x + y) \rightarrow [\nu(x) \vee \nu(y)]$.

[13] An open set is a subset of the set of all basic open, which represents formally the union of all its elements. Here $\mu(x)$ is interpreted as the subset $\{z \in \mathsf{D} \mid z \leq x\}$.

In general, it is not possible to realize effectively these conditions, i.e. to build a predicate that satisfies these conditions. However, if we require only that $\nu(x)$ is an open of a topological space, rather than a truth value, then it is possible to realize these conditions effectively.

We will define a formal space $X$ such that it is possible to realize the previous conditions by giving values for $\nu(x)$ as opens of $X$. The goal is in some sense to show the consistency of the conditions above seen as a propositional theory by building a particular topological model.

We define $Z(x)$ to mean $\exists n[x^n = 0]$, that is $x$ is nilpotent. We may expect that $\neg\nu(x)$ is provable iff $Z(x)$ holds, since classically, $x$ is nilpotent iff it belongs to all prime ideals. We define

$$x \lhd U \;=\; \forall z\ [[\forall y \in U\ Z(y\ z)] \Rightarrow Z(x\ z)].$$

This relation satisfies the following properties

- $x \lhd 1$,
- if $x \in U$ then $x \lhd U$,
- if $x \lhd U$, and $U \lhd V$, then $x \lhd V$,
- if $x \lhd U$, then $x\ y \lhd U$,
- if $x \lhd U$ and $x \lhd V$, then $x \lhd UV$,
- $x + y \lhd \{x, y\}$.

All these conditions are directly checked. Hence, we can consider a formal space whose basic neighbourhoods are the elements of $A$ and the covering relation is $\lhd$. Let $X$ be this formal space.

**Proposition:** If $1 \lhd \emptyset$ in $X$, then $1 = 0$ in $A$.

This is direct because $1 \lhd \emptyset$ means $Z(1)$, which is equivalent to $1 = 0$.

A possible reformulation of this construction is the following: if $U \subseteq A$, let $U^\perp$ be $\{x \in A \mid xU \subseteq Z\}$, where $Z$ is the radical of $A$, i.e. the set of nilpotent elements of $A$. Then $U \lhd V$ is equivalent to $V^\perp \subseteq U^\perp$ and $X$ is the locale of subsets $U$ of $A$ such that $U = U^{\perp\perp}$. That is, the formal space we consider is the space of phases defined by $A$ and $Z$.

If we interpret the proposition $\nu(x)$ as the basic open $x$ of the space $X$, all the conditions on $\nu$ are satisfied. Hence we have a model of the propositional theory describing $\nu$.

The first formal description of this space of prime ideals is due to A. Joyal.

This proposition can be used to prove that a given ideal $J$ of a ring $B$ contains 1: it is enough to show that the space $X$ of prime ideals of the quotient ring $A = B/J$ is not consistent, i.e. $1 \lhd \emptyset$. This corresponds closely to the non-effective argument: if 1 is not in $J$, then deduce a contradiction from the existence of a prime ideal that contains $J$. However, it becomes in this way an effective argument: the inconsistency of $X$ can be transformed to an actual derivation that 1 belongs to $J$.

This is this method that we shall illustrate in van der Waerden's example. Notice that we reformulate the problem of showing $1 \in J$ as the problem of showing a contradiction in a suitable theory.

## 4.6 Henkin Sets

Another suggestive example is the notion of Henkin sets. Given a first-order classical theory $T$, its Tarksi-Lindenbaum algebra is a boolean algebra. A *Henkin set* is a predicate $\mu$ on this boolean algebra which defines an ultrafilter $\mu$ such that $\mu(\exists x\ A) \rightarrow \bigvee_t\ \mu(A[t])$.

It is possible to show that the space defined by this theory, called the Henkin topology associated to $T$, is consistent if the theory $T$ is consistent. Indeed, it is enough to consider the phase space defined by $Z = \{A \mid A \vdash \perp\}$. It can be checked that this provides a model for the predicate $\mu$ above.

**Proposition:** If $1 \lhd \emptyset$ then the first-order theory $T$ is inconsistent.

**Proof:** Direct using the phase model, since $1 \lhd \emptyset$ implies $1 \in Z$, that is $1 \vdash \perp$. $\square$

This example is interesting because Henkin sets can be used to give an elegant proof of completeness [Feferman]. We have given a constructive meaning to this proof. It would be quite difficult to analyse this proof by negative translation, or by using sequent calculus.

## 4.7 Jacobson's Theorem

As a first concrete example of an elimination of the use of the Axiom of Choice, we take a simplified proof of a simple case of Jacobson's theorem.

**Theorem:** If $A$ is a ring such that $x^3 = x$ for all $x \in A$, then $A$ is commutative.

The general form is that commutativity follows from the fact that, for all $x$ in $A$, there exists $n(x) > 1$ such that $x^{n(x)} = x$.

The idea is to reduce the problem to the case where $A$ is a division algebra. In this case, the theorem is clear since $x^3 = x$ can be written $x(x-1)(x+1) = 0$ and hence implies $x = 0$ or $x = 1$ or $x = -1$. To reduce the problem to this case, we must ensure the existence of enough maximal ideals. For this, we can either classically use the axiom of choice, or alternatively, use topological models.

First, we state some lemmas that have a direct proof.

**Lemma 1:** If $x^2 = 0$, then $x = 0$.

**Proof:** we have then $x = x^2x = 0$. $\square$

**Lemma 2:** If $e^2 = e$, then $ex = xe$ for all $x$.

**Proof:** If $y = ex(1-e)$ we have $y^2 = 0$, and hence by lemma 1, $y = 0$, that is $ex = exe$. Similarly, we prove $xe = exe$. Hence $ex = xe$. $\square$

Let $B$ be the boolean algebra of all idempotents of $A$, that is, all elements $e \in A$ such that $e^2 = e$. This is a boolean algebra where the addition is defined by $e_1 +' e_2 = e_1 + e_2 - 2e_1e_2$ and the multiplication is the multiplication of $A$. Lemma 2 is needed to check that $e_1 +' e_2$ is an idempotent if $e_1, e_2$ are idempotent. Notice that $x^2 \in B$ for all $x \in A$, and hence, for all $x \in A$, there exists $e \in B$ such that $xe = ex = x$.

### 4.7.1 First proof (non effective)

What follows is a simplified version of Jacobson's proof, which uses the Axiom of Choice. If $x \neq 0$, there exists a maximal ideal $J$ on $B$ such that $x^2$ is not in $J$, that is $x$ is not in $\bar{J}$. This follows from the fact that $x^2 \neq 0$ by lemma 1.

**Lemma 3:** if $J$ is a maximal ideal of $B$, then $\bar{J} = \{x \in A \mid x^2 \in J\}$ is a double sided ideal of $A$ such that $A/\bar{J}$ is a division algebra.

**Proof:** The verification that $\bar{J}$ is an ideal involves only elementary algebraic manipulations. We give them here for sake of completeness. First, if $x^2 \in J$ we have $(xy)^2 = x^2(xy)^2$ and hence $(xy)^2 \in J$. Similarly, $(yx)^2 = (yx)^2x^2$ and hence $(yx)^2 \in J$. Thus $xy \in \bar{J}$ and $yx \in \bar{J}$ if $x \in \bar{J}$. Next, we claim that $x \in \bar{J}$ iff there exists $e \in J$ such that $xe = x$. In one direction, this follows from $xx^2 = x$. Conversely, if $e \in J$ and $xe = x$, then $x^2e = x^2$ and hence $x^2 \in J$. If $x^2 \in J$ and $y^2 \in J$, we have $x^2 \vee y^2 = x^2 + y^2 - x^2y^2 \in J$ and $(x+y)(x^2 \vee y^2) = x + y$, hence $x + y \in \bar{J}$.

Finally, we prove that the quotient $A/\bar{J}$ is a division algebra if $J$ is a maximal ideal of $B$. If $x \in A$, we have $x^2 \in J$ or $1 - x^2 \in J$. If $x^2 \in J$, then $x \in \bar{J}$. If $1 - x^2 \in J$, then $x$ is its own inverse modulo $\bar{J}$. $\square$

The quotient $A/\bar{J}$ is then a division algebra and we deduce $x = 0, 1$ or $-1$ modulo $\bar{J}$, hence the commutativity of each $A/\bar{J}$. Hence, $xy - yx = 0$ modulo each $\bar{J}$ and, by the remark above, $xy = yx$.

### 4.7.2 Second Proof (effective)

It is possible to eliminate the use the Axiom of Choice in the first argument by interpreting the proof in the topological model defined by the boolean algebra $B$, where truth values are ideals of $B$. We define $J_x = \{e \in B \mid xe = 0\}$. This is an ideal of $B$. The value of $x = y$ for $x, y \in A$ is defined as

$$[\![x = y]\!] = \{e \in B \mid xe = ye\} = J_{x-y}.$$

The following observation is the key to eliminate the use of maximal ideals.

**Transfer Principle:** If $x = y$ holds in the topological model defined by $B$, it holds in $A$.

**Proof:** If we have $[\![x = y]\!] = B$, we have $1 \in J_{x-y}$ and hence $x-y = 1(x-y) = 0$. $\square$

The following formula is true under this interpretation

$$(\forall x \in A)[x = 0 \vee (\exists y \in A)[xy = 1]]$$

indeed, this means $B = J_x + \Sigma_y J_{xy-1}$, which holds because $B = J_x + J_{xx-1}$ since $1 - x^2 \in J_x$ and $x^2 \in J_{xx-1}$. It follows first that we have

$$[ab = 0] \Rightarrow [[a = 0] \vee [b = 0]],$$

and hence, from $x^3 - x = x(x-1)(x+1) = 0$ we deduce that the following formula holds

$$(\forall x \in A)[x = 0 \vee x = 1 \vee x = -1],$$

so that

$$(\forall x, y \in A)[xy = yx].$$

This means $[\![xy = yx]\!] = B$, and so, by the transfer principle $xy = yx$ in $A$.

### 4.7.3 Third Proof (effective)

It is possible to analyse completely this proof and to get a purely equational proof.

We analyse $[\![x = 0 \vee x = 1 \vee x = -1]\!] = B$. This means that, for any $x \in A$, we can find $e_1, e_2, e_3 \in B$ such that $1 = e_1 + e_2 + e_3$ and $xe_1 = 0,\ xe_2 = e_2,\ xe_3 = -e_3$.

Indeed, the analysis gives us $e_1 = 1 - u,\ e_2 = u(1-v)$ and $e_3 = uv$ where $u = x^2$ and $v = (1-x)^2$.

Using the fact that idempotents commute with any elements (lemma 2), it follows that

$$xy = e_1xy + e_2xy + e_3xy = e_2y - e_3y = e_1yx + e_2yx + e_3yx = yx.$$

This is really in the spirit of Hilbert's program; the use of maximal ideals has disappeared, and at the end, we get even a purely equational proof.

## 4.8 Van der Waerden's Theorem

Girard, in his book "Proof Theory and Logical Complexity", analyses a proof of Van der Waerden's theorem on arithmetical progession that uses some general lemmas of topological dynamics. Van der Waerden's theorem states that if $k$ is given, there exists $N$ such that for any partition $A, B$ of $[1, N]$, either $A$ or $B$ contains an arithmetical progression of length $k$. This is a $\Pi^0_2$ statement, and it is natural to ask what is the computational content of its non-combinatorial proof. One general lemma used in this proof is the following: if $X$ is a compact space and $f : X \rightarrow X$ a continuous map, there exists $K$ compact non-empty such that $f(K) \subseteq K$ and if $L$ compact non-empty such that $L \subseteq K$ and $f(L) \subseteq L$, then $K = L$. That is there exists a *minimal* invariant closed subspace.

Girard does not directly analyse this statement, but instead gives an equivalent statement, which is possible to analyse using the method of no counterexample, yet another method of extracting computational content of non-effective proofs, which is described in detail in Girard's book. It is possible to use formal topology and to give a topological model in which such a minimal invariant subspace exists in a relative sense, at least in the case where $X$ is a *boolean* space, that is the Stone space of a boolean algebra $B$. This method provides an alternative analysis of the computational content(s) of this proof. Morever, it extracts a purely algebraic and elementary lemma that can be seen as the "formal" statement of the existence of minimal invariant subspace.

In term of the boolean algebra $B$, a minimal invariant subspace can be described as a predicate $\mu$ such that

1. $\mu(1)$,
2. $\neg\mu(0)$,
3. if $\mu(x)$ and $x \subseteq y$, then $\mu(y)$,
4. if $\mu(x)$ and $\mu(y)$, then $\mu(x.y)$,
5. if $\mu(x)$, then $\mu(g(x))$,
6. $\mu(1-x)$ or $\mu(\vee_{i\leq n} g^i(x))$ for one $n$.

Here $g$ is a morphism $B \rightarrow B$ of boolean algebras, which corresponds to a continuous map $f : X \rightarrow X$.

We can read $\mu(x)$ as "the closed open subspace $x$ of $X$ contains the closed invariant subspace $K$," where $K$ is invariant iff $f(K) \subseteq K$. Conversely, $K$ is the intersection of all elements of $B$ satisfying $\mu$. If we add the condition $\neg\mu(x)$ for $x \in I$, where $I$ is an invariant ideal of $B$, we describe a closed invariant subspace included in a given closed subspace of $X$.

Given such an ideal, we introduce the predicate $Z_I(x)$ meaning that there exists $n$ such that $\wedge_{i\leq n} g^i(x) \in I$. The next three lemmas have direct proofs.

**Lemma 1:** If there exists $n$ such that $Z_I(\wedge_{i\leq n} g^i(x))$, then $Z_I(x)$.

**Lemma 2:** If $Z_I(x)$ and $y \subseteq x$, then $Z_I(y)$.

**Lemma 3:** If $Z_I(x)$ and $y \in I$, then $Z_I(x \vee y)$.

**Proof:** Because $I$ is closed under the morphism $g$. $\square$

Notice that, a priori, we cannot conclude that $Z_I(x \vee y)$ if we know only $Z_I(x)$ and $Z_I(y)$.

The main combinatorial property is:

**Proposition 1:** If $Z_I(y.(1-x))$ and $Z_I(y. \vee_{i\leq n} g^i(x))$ for all $n$, then $Z_I(y)$.

**Proof:** We have $n$ such that $\wedge_{i\leq n} g^i(y.(1-x)) \in I$. By lemma 1, it is enough to show that $Z_I(\wedge_{i\leq n} g^i(y))$. This follows from lemmas 2, 3 and the inequality

$$\wedge_{i\leq n} g^i(y) \subseteq \wedge_{i\leq n} g^i(y.(1-x)) \vee y. \vee_{i\leq n} g^i(x).$$

This inequality is a special case of the following remark: if $w \leq u_i \vee v_i$ for all $i$, then $w \leq \wedge u_i \vee \vee v_i$. We apply this remark to the case $w = \wedge_{i\leq n} g^i(y)$ and $u_i = g^i(y.(1-x)),\ v_i = y.g^i(x)$. $\square$

We introduce next a covering relation on the set $B$

$$x \lhd U \ = \ (\forall z)[[(\forall y \in U) Z_I(z.y)] \Rightarrow Z_I(z.x)].$$

This defines a formal space $\mathsf{M}$, following Sambin's definition of a formal topology [Sambin].

**Proposition 2:** The relation $x \lhd U$ satisfies

- if $x \in U$, then $x \lhd U$,
- if $x \lhd U$, and $U \lhd V$, then $x \lhd V$,
- if $x \lhd U$ and $x \lhd V$, then $x \lhd UV$,
- if $x \lhd U$ then $x.y \lhd U$,
- $x \lhd g(x)$,
- $1 \lhd 1 - x, \bigvee_n \vee_{i\leq n} g^i(x)$.

**Proof:** The first three conditions do not use any special properties of the predicate $Z_I$.

The fourth condition follows from lemma 2.

It is clear that if $Z_I(z.g(x))$, then $Z_I(z.x)$ and hence $x \lhd g(x)$.

The last condition follows from proposition 1. $\square$

We can use the previous construction to give a topological model of the predicate $\mu$ described above. For this, we interpret each proposition $\mu(x)$, for $x \in B$, as an open of the formal space $\mathsf{M}$, namely as the basic open $x$. It can then be checked that all six properties characterising the property $\mu$ get interpreted by the open 1. Furthemore the condition $\neg\mu(x)$ holds for $x \in I$. This is used in [Coquand] in the proof-theoretical analysis of the topological proof of van der Waerden's theorem on arithmetical progression. In this case, the boolean algebra $B$ is the Tarski-Lindenbaum algebra on countably many atomic propositions $A_n$ and $g$ is defined as the shift morphism $g(A_i) = A_{i+1}$.

As for the example of the spectrum of a ring, a possible reformulation of this construction is the following: if $U \subseteq B$, let $U^\perp$ be $\{x \in B \mid xU \subseteq Z_I\}$, where $Z_I$ is the set of elements $x$ such that $\wedge_{i\leq n} g^i(x) \in I$ for some $n$. Then $U \lhd V$ is equivalent to $V^\perp \subseteq U^\perp$ and $X$ is the locale of subsets $U$ of $B$ such that $U = U^{\perp\perp}$. That is, the space we consider is the space of phases defined by $B$ and $Z_I$.

# Conclusion

In conclusion, we have given four different instances of uses of spaces of phases: for the spectrum of a distributive lattice, for the spectrum of a ring, for the space of Henkin sets, and finally for the space of minimal invariant subspaces. The use of formal topology in the example of Jacobson's theorem was of a different nature: we were using the space defined by the boolean algebra of idempotents of a ring.

## 4.9 References

[ML68] P. Martin-Löf *Notes on Constructive Mathematics.* Almqvist & Wiksell ed. The theory of the continuum by Brouwer can be described as a non-atomistic theory of non-discrete space. For instance Cantor space is not defined as a *set* of points, but as a spread. This is clearly explained in this book.

[Stone] P.J. Johnstone, *Stone Spaces*, Cambridge Studies in Advanced Mathematics

The introduction to the theory of locales. Contains the basic results and interesting references. In particular, the paper "The point of pointless topology", BAMS, is quite suggestive.

[ML83] P. Martin-Löf "Domain Interpretation of Type Theory" Workshop on the semantics of Programming Languages, Chalmers 1983

A very clear proof of the adequacy theorem for denotational semantics that connects it with operational semantics.

[Scott82] D. Scott "Domains for denotational semantics." Proceeding of ICALP 82, LNCS 140.

Presents the notion of information systems, that can be seen as a point-free presentation of domains.

[Tsao] Tang Tsao-Chen "Algebraic Postulates and a Geometric Interpretation for the Lewis Calculus of Strict Implication." BAMS 44 (1938), p. 737-744.

A clear geometric view of modal operators.

[Vickers89] S. Vickers, *Topology via Logic*, Cambridge Tracts in Theoretical Computer Science 5

Contains some connections between the theory of locales and domain theory.

[Wiener14] N. Wiener, "A Contribution to the Theory of Relative Position." Proc. Camb. Phil. Soc., Vol. 17

[Russell14] B. Russell, *Our Knowledge of the External World*, Cambridge Universtity Press.

[Whitehead19] A.N. Whitehead, *The Concept of Nature*, Cambridge Universtity Press.

[Russell36] B. Russell, "On order in time." In Logic and Knowledges, essays 1901-1950, R.C. Marsh editor.

Early references to the work in "point-free topology". Suggests some intriguing connections with physics.

[Moore35] R.L. Moore, Fundamenta Mathematicae 25.

Contains a point-free presentation of the plane.

[Menger40] K. Menger "Topology without Points." Rice Institute Pamphlet.

In this survey, a large part is concerned with the construction of points from what Menger calls "lumps", that can be thought as basic neighbourhoods (Moore uses the terminology "pieces"). Let us cite Menger: "Such a topology of lumps seems to me closer to the physicist's concept of space than is the point set theoretical concept. For naturally all the physicist can measure and observe are pieces of space, and the individual points are merely given as the result of approximations."

[Weyl] H. Weyl "Ueber die neue Grundlagenkrise der Mathematik", Mathematische Zeitschrift, 10, 1921.

This text contains an early presentation of the basic notions of first-order logic (H. Weyl's thesis was about trying to explain Zermelo's formalisation of set theory, and he introduces these notions for this purpose; this later inspired Skolem), and the idea that an existential statement can be seen as an incomplete statement (an idea that was taken up in Hilbert-Bernays, and later motivated Kleene in formulating his realizability interpretation). It contains also a point-free definition of reals, continuous functions, and a sketch of a point-free definition of the notion of manifolds.

[Mostowski] A. Mostowski. "Proofs of non-deducibility in intuitionistic functional calculus." Journal of Symbolic Logic 13, p. 204-207, 1948

First presentation of topological models for first-order logic. (Formulae are interpreted by closed subsets!) It is used to show the non derivability of some formulae (we present similar examples in the appendix). The completeness of this method is conjectured.

[Mulvey] Ch. Mulvey, J.W. Pelletier. "A Globalization of the Hahn-Banach Theorem." Advances in Mathematics, Vol. 89, p. 1-59, September 1991

Ch. Mulvey, J.W. Pelletier. "A geometric characterization concerning compact, convex sets." Math. Proc. Camb. Phil. Soc. , 109, p. 351-361, 1991

Quite elegant presentation of some basic results of functional analysis in a localic framework.

[Vermeulen] J. Vermeulen, Ph.D. Thesis.

Contains an elegant formal presentation of reals and an intuitionistic proof of a localic version of Hahn-Banach, to be contrasted with Mulvey's paper, which presents the localic version, but proves it using Barr's theorem.

[Sambin87] G. Sambin. "Intuitionistic Formal Spaces - a first communication." In Mathematical Logic and its applications, D. Skordev ed., Plenum, 187-204.

[Dragalin87] A. Dragalin, two papers presented in the same volume where Sambin's paper appeared: Mathematical Logic and its applications, D. Skordev ed.

A formal space is given here as a partial order with a covering relation. This is closer to the notion of coverage presented in [Vickers] and [Stone].

[Sambin 93] G. Sambin "The semantics of pretopologies", in: "Substructural logics", ed. P. Schroeder-Heister - K. Dosen, Clarendon, Oxford 1993, p. 293-307

[Sambin 95] G. Sambin "Pretopologies and completeness proofs", J. Symbolic Logic 60 (1995), p. 863-878

[Feferman] review of Rasiowa-Sikorski, JSL 17, p. 72.

A quite clear presentation of a topological proof of completeness for first-order logic.

[Ceder] J. Cederquist "A machine assisted formalization of pointfree topology in type theory." Technical Report, Chalmers University.

A beginning of a complete formalisation of pointfree topology in type theory. Contains still another alternative to the presentation of formal spaces.

[Coquand] Th. Coquand and J. Smith "An application of Constructive Completness," to appear in the proceeding of the meeting Proof and Types, Torino 1995.

This is an application of formal spaces to give a constructive proof of a conservativity result, inspired by Dragalin's use of topological models.

Th. Coquand "Minimal Invariant Spaces in Formal Topology."

To appear in the Journal of Symbolic Logic. Shows that the localic version of the existence of minimal invariant subspaces can be applied in the same way as the usual existence in the topological proof of van der Waerden's theorem on arithmetical progression.

# 5 Appendix: Boolean Models

We present the basic definitions and some applications of the notion of boolean models: non derivability of Markov's principle, of the axiom of choice in some systems, and a new proof of Herbrand's theorem. The general idea is to replace the truth-value 0,1 by ideals of a fixed boolean algebra $B$. This is a special case of topological models. As usual, we denote by $I + J$ the ideal generated by $I \cup J$, while $\Sigma I_\alpha$ denotes the ideal generated by the union of all ideals $I_\alpha$.

The notion of boolean models in metamathematics goes back to Tsao-Chen, Stone and Tarski (for modal and propositional logic) and Mostowski (for first-order logic). One important and new point is that we can define and use this notion in an effective way, without using indirect reasoning. All the proofs that follow are effective, and indeed, can be represented in Intuitionistic Type Theory.

## 5.1 Semantics of First-Order Logic

### 5.1.1 Intuitionistic First-Order Logic

We suppose given an interpretation $[\![P]\!] : \mathsf{D}^k \rightarrow \mathsf{B}$, for each atomic $k$-ary predicate $P$, and an interpretation $[\![f]\!] : \mathsf{D}^k \rightarrow \mathsf{D}$ of each $k$-ary function symbol $f$. We can then interpret $[\![t]\!]_\rho \in \mathsf{D}$ and $[\![\phi]\!]_\rho$ as an ideal of $\mathsf{B}$. For $\phi = P\ t_1 \dots\ t_k$ $[\![\phi]\!]_\rho$ is the principal ideal generated by $[\![P]\!]\ [\![t_1]\!]_\rho \dots\ [\![t_k]\!]_\rho$. We define $[\![\exists x\ \phi]\!]_\rho$ to be $\Sigma_{d \in \mathsf{D}}\ [\![\phi]\!]_{(\rho, x=d)}$ and $[\![\forall x\ \phi]\!]_\rho$ to be $\bigcap_{d \in \mathsf{D}}\ [\![\phi]\!]_{(\rho, x=d)}$. Notice that with this definition, each atomic formula is intended to be decidable. It would be possible to give a more general definition of models without this hypothesis, by requiring only to assign an ideal of $B$ to each atomic proposition.

### 5.1.2 Classical First-Order Logic

In order to get an interpretation of classical logic, we define first a negation operator on ideals of $B$: if $I$ is an ideal, then $I^\perp$ is the ideal of $x \in B$ such that $xy = 0$ for all $y \in I$. It is then clear that $I^{\perp\perp}$ is an ideal that contains $I$, for any ideal $I$ of $B$. We call an ideal $I$ *regular* iff it is such that $I = I^{\perp\perp}$.

**Proposition 1:** We have the following properties

1. an intersection of an arbitrary family of regular ideals is a regular ideal,
2. for any ideal $I$, the ideal $(I + I^\perp)^\perp$ is the zero ideal 0,
3. any principal ideal is regular.

These assertions have a direct proof. We define then

$$[\![\exists x\ \phi(x)]\!] = (\Sigma_{d \in D} [\![\phi(d)]\!])^{\perp\perp}$$

and

$$[\![\phi \vee \psi]\!] = ([\![\phi]\!] + [\![\psi]\!])^{\perp\perp},$$

By the first property above, we can define:

$$[\![\forall x\ \phi(x)]\!] = \bigcap_{d \in D} [\![\phi(d)]\!].$$

and by the second property, we see that the law of excluded middle $\phi \vee \neg\phi$ is valid.

We say that such a model is a model of a theory $T$ iff $[\![\psi]\!]$ is the principal ideal 1 for all $\psi \in T$. The following soundness property is proved directly by induction.

**Proposition 2:** If $\phi$ is provable in a theory $T$, then for any model of $T$, we have $[\![\phi]\!] = 1$.

## 5.2 Applications

### 5.2.1 Markov's principle

We consider the boolean algebra $\mathsf{B}$ generated by a countable number of elements $A_0, A_1, \ldots$.[14] Notice that any element $x \in \mathsf{B}$ "depends only on" a finite number of elements $A_i$. In particular if $x$ is not 0, there are only finitely many $i$ such that $x \leq A_i$ or $x \leq \neg A_i$. Thus, if $x \leq A_i$ or $x \leq \neg A_i$ for all $i$, then $x = 0$.

Over this boolean model, we can find a decidable predicate $\alpha$ such that the value $[\![\neg\neg\exists n\ (\alpha\ n)]\!]$ is 1 and $[\![\exists n\ (\alpha\ n)]\!]$ is not 1. Indeed, we can take $\alpha\ n = A_n$. Then, $[\![\neg\neg\exists n\ (\alpha\ n)]\!]$ is $(\bigcap_n A_n^{\perp})^{\perp}$. But we have just seen that $\bigcap_n A_n^{\perp} = 0$ and hence $[\![\neg\neg\exists n\ (\alpha\ n)]\!]$ is 1. Next, $[\![\exists n\ (\alpha\ n)]\!]$ is $\Sigma A_n$, which is not the ideal 1 since, for instance, $\neg A_{27}$ does not belong to the ideal $\Sigma A_n$.

Mostowski introduced topological models of first-order intuitionistic logic in order to show the non derivability of some formulae. However, a crucial difference is that he was using a non effective metalanguage.

### 5.2.2 Herbrand's Theorem

As another application of Boolean models, here is a constructive proof of Herbrand's theorem. Let $\exists x\ A$ be a provable formula, with $A$ quantifier-free. We let $C$ be the usual Tarski-Lindenbaum boolean algebra of formulae, and $I$ the ideal of $C$ generated by all instantiation $A(t)$, for $t$ term. Let $B$ be the quotient algebra $C/I$.

We define a boolean model whose domain is the set $D$ of terms, and by interpreting an atomic formula $P(t_1, \ldots, t_n)$ by the formula $P(t_1, \ldots, t_n)$ itself modulo $I$. Then $[\![\exists x\ A]\!]$ is 0 because each $A(t)$ gets the value 0 and each $[\![A]\!]_{x=t}$ is equal to $A(t)$ since $A$ is quantifier-free.

Hence $0 = 1$ in $B$, that is $1 \in I$ in C, and there exists a finite number of terms $t_1, \ldots, t_k$ such that $A(t_1) \vee \ldots \vee A(t_k)$ is provable.

## 5.3 Semantics of Analysis

### 5.3.1 The language of Analysis

We give a model of $\mathsf{HA}^{\omega}$. The interpretations of terms are defined as usual, while the interpretations of formulae will be ideals of a fixed-boolean algebra. We can

[14] The algebra $\mathsf{B}$ can also be described as the unique countable atomless boolean algebra.

interpret $\mathsf{HA}^\omega + \mathbf{EM}$ by interpreting formulae as regular ideals.

### 5.3.2 Application to the Axiom of Choice

We exhibit a boolean model in which the formula

$$\exists f\ \forall n\ [[f\ n = 0] \equiv \alpha\ n]$$

is interpreted by the ideal 0. The boolean algebra we use is the boolean algebra $\mathsf{B}$ generated by $A_0, A_1, \ldots$ We interpret $\alpha\ n$ as the principal (and hence regular) ideal generated by $A_n$. The ideal $\exists f\ \forall n\ [[f\ n = 0] \equiv \alpha\ n]$ is then

$$\Sigma_f \bigcap_n [\![ [f\ n = 0] \equiv \alpha_n ]\!].$$

But I claim that, for each given $f : \mathsf{N} \to \mathsf{N}$, the interpretation of $\bigcap_n [\![ [f\ n = 0] \equiv \alpha_n ]\!]$ is 0. Indeed, for a given $n$, the interpretation $[\![ [f\ n = 0] \equiv \alpha_n ]\!]$ is $A_n$ if $f\ n = 0$ and $\neg\ A_n$ if $f\ n \neq 0$. The assertion follows then from the fact that if $x \leq A_n$ or $x \leq \neg A_n$ for all $n$, then $x = 0$ in $\mathsf{B}$.