16w5099—INTERVAL ANALYSIS AND CONSTRUCTIVE MATHEMATICS

Douglas Bridges (University of Canterbury), Hannes Diener (University of Canterbury),
Baker Kearfott (University of Louisiana at Lafayette),
Vladik Kreinovich (University of Texas at El Paso),
Patricia Melin (Tijuana Institute of Technology),
Raazesh Sainudiin (University of Canterbury),
Helmut Schwichtenberg (University of Munich)

13–18 November 2016

1 Overview of the Field

1.1 Constructive Mathematics

In this case, we have two fields to overview—constructive mathematics and interval analysis—one of the main objectives of the workshop being to foster joint research across the two.

By 'constructive mathematics' we mean 'mathematics using intuitionistic logic and an appropriate set- or type-theoretic foundation'. Although the origins of the field go back to Brouwer, over 100 years ago, it was the publication, in 1967, of Errett Bishop's *Foundations of Constructive Analysis* [16, 17] that began the modern revival of the field. Bishop adopted the high-level viewpoint of the working mathematical analyst (he was already famous for his work in classical functional analysis and several complex variables), and developed constructively analysis across a wide swathe of the discipline: real, complex, and functional analysis, as well as abstract integration/measure theory. The significant aspect of his work is that the exclusive use of intuitionistic logic guaranteed that each proof embodied algorithms that could be extracted, encoded, and machine-implemented. For a rather simple example, Bishop's proof of the fundamental theorem of algebra is, in effect, an algorithm enabling one to find the roots of a given complex polynomial; contrast this with the standard undergraduate proofs, such as the *reductio ad absurdum* one using Liouville's theorem.

The succeeding 40 years have seen Bishop's work continued in those parts of analysis he dealt with, as well as developments in other parts of the subject: partial differential equations, algebra, topology, mathematical economics, ... On the other hand, much has been accomplished towards establishing Bishop-style constructive mathematics (**BISH**) on firm foundations: witness the type-theory of Martin-Löf [55] and several set theories, such as the constructive Zermelo-Fraenkel of Aczel and Rathjen [2], and the constructive Morse set theory of Alps and Bridges [4]. In addition, several groups in mathematics and computer science departments have made major strides towards the extraction, and subsequent implementation, of programs from constructive proofs; among those groups are the long-active Cornell one led by Constable [26], and that of Schwichtenberg in Munich [11] (representatives of each of those two groups spoke at the workshop). Related research in domain theory and other areas has also proved fruitful, and was presented by Blanck and others in Oaxaca.

1.2 Interval Analysis

Classical interval mathematics is based on interval arithmetic, in which arithmetic operations are defined on ordered pairs of numbers $\mathbf{x} = [\underline{x}, \overline{x}]$, with a *lower bound* $\underline{x}$ and an *upper bound* $\overline{x}$, where the result of an operation $\mathbf{x} \odot \mathbf{y}$ on two intervals $\mathbf{x}$ and $\mathbf{y}$ is the range

$$\{x + y \mid x \in \mathbf{x} \text{ and } y \in \mathbf{y}\}\,.$$

(See, for example, [58] or any of the numerous other introductory texts on the subject.) The power of interval mathematics lies in the fact that if $E : \mathcal{D} \subseteq \mathbb{R}^n \to \mathbb{R}$ is an expression of n variables $x \in \mathbb{R}^n$, evaluating E over an interval $\mathbf{x}$ gives

$$\{E(x) \mid x \in \mathbf{x}\} \subseteq \mathbf{E}(\mathbf{x}), \tag{1}$$

where $\mathbf{E}(\mathbf{x})$ is the interval evaluation of E with interval argument $\mathbf{x}$. In general, the inequality in (1) is not sharp.

This idea surfaced many times, starting in the nineteenth century, but became widely visible with Ramon Moore's dissertation [57]; see

http://interval.louisiana.edu/Moores_early_papers/bibliography.html

for a posting of some of Moore's early work.

In a modern setting, interval arithmetic can be implemented on the vast majority of current computers in such a way that it can be used to provide mathematically rigorous proofs. For example, in IEEE-754 floating point arithmetic [38], the result of a computer operation $\mathbf{x} \odot \mathbf{y}$ can be either rounded down to the nearest machine number less than the actual result, or else rounded up to the nearest machine number greater than the actual result. This provides an assurance that, even when E is evaluated using the approximate machine arithmetic, the interval value $\mathbf{E}(\mathbf{x})$ is guaranteed to contain the actual range of E over $\mathbf{x}$.

Such machine interval arithmetic can be used in various ways to effect mathematical proofs. In particular, various existence and uniqueness results can be posed in terms of a fixed point equation $x = G(x)$, where the existence (and, in some cases, the uniqueness) can be proved by showing that $\mathbf{G}(\mathbf{x})$, the range of G over $\mathbf{x}$, is a subset of $\mathbf{x}$. Other proofs, such as proof of stability of an equilibrium of a dynamical system, depend on showing that a certain expression $E(x)$ has $E(x) > 0$, something that can be done with interval arithmetic.

Two examples from among the many important open mathematical problems that have been solved with the aid of interval arithmetic are the proof of the Kepler conjecture [36] and the proof that the Lorenz equations support a strange attractor (Smale's 14th problem) [78].

Interval arithmetic is closely tied to the philosophical underpinnings of constructive mathematics, since proofs involving interval arithmetic consist precisely of constructing, implementing, and running an algorithm to produce an object. Computer-aided proofs involving interval arithmetic can involve computer programs with extensive symbolic logic. To ensure that proofs are constructive, interval arithmetic experts must avoid certain classical-logical steps, such as using $\neg(\neg A \wedge \neg B)$ to prove $A \vee B$. Extensive exposure of interval experts to constructive symbolic logic and variants during the meeting enabled the attending interval experts to tailor their software to these particular systems.

2 Recent Developments and Open Problems

2.1 Constructive Mathematics

Analysis One of the most highly nonconstructive areas of classical analysis is the theory of operator algebras, which is riddled with existence proofs of the pattern: suppose the object in question does not exist, apply Zorn's lemma to construct a maximal family of a certain type, derive a consequent contradiction, and conclude that the desired object exists after all. Although many classical proofs-by-contradiction provide clues about how one can prove constructive counterparts, ones that use the operator-algebra proof style leave the constructive analyst clueless. It was therefore highly impressive that Spitters, in his Nijmegen doctoral thesis in 2002 (see [75]), proved the von Neumann double commutant theorem in the case where the operator algebra was commutative; but the non-commutative case remains open. In 2010, Bridges produced a constructive counterpart of the classical characterisation of weak-operator continuous linear functionals on $\mathcal{B}(H)$, the algebra of bounded linear operators on a Hilbert space H; his proof requires explicitly stronger hypotheses than the classical one, which reflects the need for more computational input in order to obtain significant computational output.

A salient feature of constructive analysis is that whereas the supremum and infimum of a uniformly continuous, real-valued function on a compact metric space exist, they need not be attained:, if even every real-valued, linear mapping of $[0,1]$ attains its supremum, then we can derive a weak sequential, but still non-constructive, form of the law of excluded middle. In fact, the classical least-upper-bound principle, the basis of the classical existence of supremum of functions, implies the full law of excluded middle (LEM). Thus in many situations in which the attainment of a supremum or infimum is granted to the classical mathematician by the least-upper-bound principle, the constructive mathematician has to use considerable ingenuity in order to establish its existence. A particularly pervasive case of this occurs with the property of locatedness. A subset S of a metric space (X,ρ) is *located* if the distance

$$\rho(x,S) \equiv \inf\{\rho(x,s) : s \in S\}$$

exists for each x in X. Many a constructive theorem depends on some set being located, either by hypothesis or else by a part of the main proof. Several results involving locatedness have been established by Ishihara et al. For example, he, Bridges, and Spitters gave conditions that ensure the locatedness of the range of an operator with an adjoint on a Hilbert space [23]. He also gave a condition equivalent to locatedness for an inhabited convex subset of a Hilbert space [40]; he and Vîţă lifted this equivalence into the context of a uniformly smooth normed space, under the additional hypothesis that the convex subset be bounded [45]. Together with Bridges, those two proved that if C is an inhabited, bounded, weakly totally bounded convex subset of a normed space X, and f is a uniformly differentiable, convex, real-valued mapping on C that is bounded below, then $\inf f$ exists; this led to a proof that if H is a Hilbert space and $\mathcal{A}$ an inhabited subset of $\mathcal{B}(H)$ that is uniformly bounded, weak-operator totally bounded, and convex, then $\mathcal{A}$ is strong-operator located in $\mathcal{B}(H)$; in particular, the unit ball of $\mathcal{B}(H)$ is strong-operator located [22] (a result proved earlier by Spitters).

Combined work of Ishihara and Richman [40, 67] showed that a bounded operator T on a Hilbert space H has an adjoint if and only if the image of the unit ball under T is located in H. Ishihara and Bridges proved the closed range theorem: if an operator with an adjoint on a Hilbert space H has closed range, then the range and kernel of T are located, and the range adjoint of T is closed [21].

Recently, Berger and Svindland have proved that every quasi-convex, uniformly continuous, positive-valued function f on a compact convex subset of $\mathbf{R}$ has positive infimum [7]. This theorem led them to a new constructive separation theorem for convex subsets of $\mathbf{R}^n$, and to the constructive content of the fundamental theorem of asset pricing in financial mathematics.

Topology There have been at least four approaches to constructive topology over the last 30 years. The oldest and most developed is *formal topology*, which was introduced by Sambin and Martin-Löf in the mid-1980s [70], in order to provide a theory of topology based on the latter's type theory. Formal topology has the distinction of being 'point free'; in other words, the emphasis is shifted from sets as collections of points, to two fundamental notions:

– a preordered set $(A,\leq)$ of *basic neighbourhoods*, and

– a *covering relation* $\lhd$ between elements of A and subsets of A,

These notions satisfy four simple axioms. Although points do not have the same status as they have in classical topology, they can be introduced as special types of subset of A; roughly, a point is identified with the set of all its neighbourhoods.

Formal topology has burgeoned in the 21st century, and has found applications in many areas of 'point-free' analysis. One appealing feature of formal topology is that it is a logically predicative theory. A major treatise on the subject by Sambin is close to publication [72].

A second approach to constructive topology, due to Bridges and Vîţă [25], is based on a primitive notion $\bowtie$ of *apartness* between subsets of the ambient *apartness space* X. From a classical point of view, apartness is the negation of the notion of proximity that is the foundation of the theory of proximity spaces [60]. The apartness relation on X must satisfy five relatively natural axioms, which lead to a substantial theory in its own right (and to a new proof-technique), with uniform spaces as its main model. The connection between apartness spaces and formal topologies is sketched in the appendix of [25].

The third approach was suggested by Bishop [16], resurrected in a paper by Bridges [19], and substantially developed by Petrakis since 2011. The fundamental notion here is that of a *function space*, comprising a set X together with a set $\mathcal{F}$ of real-valued functions on X that satisfies four axioms capturing what we would expect of the continuous functions on a classical topological space. Petrakis has shown how to fit, or reflect, within this framework a considerable body of classical point-set topology, including even such things as the Stone-Čech compactification [59, 61, 62]

The fourth approach also goes back to Bishop, and is perhaps the closest in spirit to classical topology. The fundamental notion this time a that of a *neighbourhood space*: a set X endowed with a family $\mathcal{N}$ of *neighbourhoods* such that if U_1 and U_2 belong to $\mathcal{N}$ and $x \in U_1 \cap U_2$, then there exists $U_3 \in \mathcal{N}$ such that $x \in U_3 \subset U_1 \cap U_2$. Neighbourhood spaces seem to be of less interest to researchers than the other three constructive approaches to topology, but Ishihara [43] et al. have discussed the connection between (quasi-)apartness spaces and neighbourhood spaces, and he alone has connected function spaces to neighbourhood ones [44].

Algebra Errett Bishop was the supervisor of J. Tennenbaum for his PhD thesis *A constructive version of Hilbert's basis theorem* (UC San Diego, 1973), which introduced a novel approach to the Noetherian condition for rings. Around that time, Richman began his investigations into constructive algebra with fundamental papers on countable abelian p-groups [65] and Noetherian rings [66]. He, Mines, and Ruitenburg subsequently gathered their work into the book [56], an algebraic counterpart to Bishop's 1967 analysis monograph [16] (see also [17]). More recently, Lombardi [53] and Yengui [79] have published monographs that have substantially extended the frontiers of constructive algebra (see also the survey [29]).

One problem with constructive algebra is that, so far, it depends heavily on the equality of the algebraic structure being discrete: that is, we can decide whether any two elements of the structure are equal. For example, the classical theory of real closed fields has been developed in the setting of discrete structures, where a sign test is available [18, 31, 52]. Thus there remains open the field of real algebra, without the discreteness condition on equality. A related important challenge is a constructive theory of o-minimal structures: a striking and powerful extension of the theory of real closed fields [32, 28]. However, some steps have been taken in this direction, leading to a constructive version of 17th Hilbert's problem for the real number field [31, 35, 52] and the introduction of virtual real roots of monic real polynomials [35, 30]. See also [68] for a discussion about the use of dependent choice in real algebra.

Constructive reverse mathematics The Friedman-Simpson program of (classical) *reverse mathematics* is a formal mathematics using classical logic and assuming, in its base system, a very weak set existence axiom. Its main question is "Which set-existence axioms are needed to prove the theorems of ordinary mathematics?", and many theorems have been classified by set-existence axioms of various strengths. Since classical reverse mathematics is formalised with classical logic, we cannot therein

- classify theorems in intuitionistic mathematics or in constructive recursive mathematics which are inconsistent with classical mathematics (for example, the continuity of mappings from the Baire space into the natural numbers);
- distinguish theorems from their contrapositions (for example, the fan theorem from the weak König lemma).

The purpose of *constructive reverse mathematics* is to classify various theorems in intuitionistic, constructive recursive, and classical mathematics by logical principles, function existence axioms, and their combinations. This classification involves finding logical principles and/or function existence axioms which are not only sufficient, but also necessary, to prove the theorems in a fairly weak formal system.

Bishop's constructive mathematics is a logically informal mathematics using intuitionistic logic and assuming some function existence axioms: the axiom of countable choice, the axiom of dependent choice, and the axiom of unique choice. It is a constructive core of the varieties of mathematics in the sense that it can be extended not only to intuitionistic mathematics (by adding the principle of continuous choice and the fan theorem) and constructive recursive mathematics (by adding Markov's principle and the extended Church's thesis), but also to classical mathematics practiced by most mathematicians today (by adding the principle of the excluded middle).

We illustrate the formal program of constructive reverse mathematics by some work of Ishihara et al. In **BISH** the existence of binary expansions of real numbers in the unit interval,

BE: Every real number in $[0, 1]$ has a binary expansion,

and the *intermediate value theorem*,

IVT: If $f : [0, 1] \to \mathbf{R}$ is a uniformly continuous function with $f(0) < 0 < f(1)$, then there exists $x \in [0, 1]$ such that $f(x) = 0$,

each imply the *lesser limited principle of omniscience* (LLPO or Σ^0_1-DML):

$$\forall_{\alpha,\beta}(\neg(\exists n(\alpha(n) \neq 0) \wedge \exists n(\beta(n) \neq 0)) \to \neg\exists n(\alpha(n) \neq 0) \vee \neg\exists n(\beta(n) \neq 0))$$

which is an instance of De Morgan's law (DML). The *weak König lemma*:

WKL: Every infinite tree has a branch,

also implies LLPO. Ishihara et al. have shown that BE and IVT follow from WKL, and hence that BE and IVT lie between WKL and LLPO; and that with countable choice—and therefore over **BISH**—LLPO implies WKL so that BE, IVT, LLPO, and WKL are equivalent over **BISH**.[1]

Many mathematical theorems equivalent to LLPO over **BISH** are equivalent to WKL over the base system $\mathbf{RCA}_0$ of classical reverse mathematics, one such theorem being the Cantor intersection theorem (CIT), a classical contrapositive of the Heine-Borel theorem. Therefore BE and IVT can be distinguished among theorems which are equivalent to LLPO in **BISH**:

$$\textbf{BISH} \vdash \text{ LLPO} \longleftrightarrow \text{ BE} \longleftrightarrow \text{ IVT } \longleftrightarrow \text{ WKL } \longleftrightarrow \text{ CIT}$$

In $\mathbf{RCA}_0$ we cannot compare theorems, such as BE and IVT, that are provable in that system. On the other hand, since **BISH** is an informal mathematical framework, we cannot compare BE and IVT with WKL in **BISH**. If we use a theory $\mathbf{T}$ for constructive reverse mathematics that is contained both in **BISH** and in $\mathbf{RCA}_0$, then we can classify BE and IVT, and compare them with WKL. Note that WKL is equivalent, over such a theory $\mathbf{T}$, to LLPO and a weak form of the axiom of countable choice. Within their base formal system $\mathbf{EL}_0$, Ishihara et al. have shown that, and by how much, BE is weaker than IVT, and IVT is weaker than CIT.

In addition to many papers on formal constructive reverse mathematics (see, for examples, [5, 41, 42, 51]), there is a body of research in informal constructive reverse mathematics: examining equivalences and implications between theorems in **BISH** supplemented by additional principles such as versions of Brouwer's fan theorem, but working in the informal style of Bishop's original analysis book. For example, Berger and Bridges [6] have shown that the anti-Specker principle $\mathbf{AS}_{[0,1]}$, classically equivalent to the essentially nonconstructive sequential compactness of the interval $[0, 1]$, is equivalent, over **BISH**, to the fan theorem for c-bars. It has also been shown, by Berger and others, that the uniform continuity theorem,

UC Every pointwise continuous, real-valued function on $[0, 1]$ is uniformly continuous,

lies between the fan theorem for Π^1_0-bars and the fan theorem for c-bars. It is an open problem in formal constructive reverse mathematics whether those two fan theorems and UC are actually equivalent over **BISH**.

[1] In the classical Friedman-Simpson program, the base system $\mathbf{RCA}_0$—a subsystem of second order arithmetic with a very weak axiom of countable choice—suffices for proving both BE and IVT, but does not prove WKL.

Program extraction from proofs Program extraction from proofs originates in a correspondence between constructive proofs and algorithms known as the *BHK-interpretation of intuitionistic proofs*; the name recognises Brouwer, Heyting, and Kolmogorov, the mathematicians who first studied the interpretation systematically. In computer science it is mostly referred to as the *Curry-Howard correspondence* or the *proofs-as-programs paradigm*. In constructive type theory, a modern incarnation of constructive mathematics due to Martin Löf [55], which is implemented in well-known proof assistants such as NuPrl [26, 15], Coq [27], and Agda [**?**], this correspondence is even an isomorphism: proofs are *identified* with programs.

A slightly different approach to capturing the algorithmic content of constructive proofs is based on Kleene's realizability [47]: to every arithmetical statement A one defines when a program, coded by a number e, *realizes* A—that is, solves the algorithmic problem expressed by A. For example, if A is of the form $\forall_x \exists_y B(x, y)$ where $B(x, y)$ is a decidable relation, then a realizer of A is (the code of) a function f that computes for every x some $y = f(x)$ such that $B(x, y)$ holds. The fundamental *soundness theorem of realizability* states that from every intuitionistic (that is, constructive) proof one can extract a realizer of the proven formula together with a formal proof of the realizing property. In computer science terms this means that from a constructive proof of a specification one can extract a program provably satisfying the specification.

Realizability as a method for program extraction[2] is implemented in many of the major constructive proof assistants, but is probably most developed in the Minlog system [54, 11, 74]. Minlog's realizers are not program codes, but functionals of (possibly) higher-types as proposed by Kreisel [49] in his *modified realizability*. In other systems, for example NuPrl, realizers are untyped elements of a partial combinatory algebra.

Program extraction has been applied in a variety of fields, for example lambda-calculus (normalization-by-evaluation [9]), polynomial time computability (non-size-increasing computations [**?**]), graphs and infinitary combinatorics (Warshall's algorithm, Dickson's Lemma, Higman's Lemma [14, 73]), Satisfiability testing (extraction of a SAT-solver [10]), and constructive analysis (see below).

A related line of research with a slightly different focus is based on Gödel's Dialectica (or Functional) Interpretation [33] and its monotone variant introduced by Kohlenbach [48]. In this approach one does not extract programs solving algorithmic problems exactly, but 'mines' proofs for bounds in approximation, fixed point-, and ergodic-theory.

Recently, algorithmic aspects of constructive analysis [16, 17, 24] have been the subject of considerable interest to the program extraction community. Realizibility interpretations of co-inductive definitions (predicates defined as largest fixed points of monotone operators) provide an elegant approach to co-algebraic data structures and hence lazy stream representations of real numbers. Program extraction has been applied successfully to obtain exact and provably correct implementations of translations between different real number representations, basic arithmetic operations, integration, and variants of the intermediate value theorem.

A particular challenge poses the formalization and realizability interpretation of Tsuiki's infinite Gray code for real numbers [77]. This is due to its inherent partiality and the resulting non-deterministic nature of algorithms processing it. Capturing these phenomena through realizability is ongoing work.

2.2 Interval Analysis

From the mid-1960s to the present, interval-analysis experts have been producing and refining both low-level software systems for interval arithmetic and higher-level systems that compute mathematically rigorous bounds to various quantities. While there are many historical systems, important systems currently in use include Rump's Intlab [69], various C++ implementations, and emerging implementations in newer languages such as Java and Python. A partial list of such packages is available on the interval-related web site maintained by Kreinovich, at

http://www.cs.utep.edu/interval-comp/intsoft.html.

In 2015, the IEEE-1788 Standard for Interval Arithmetic [39] became available. Besides specifying interpretation and behaviour of operations for unbounded intervals (such as $[1, \infty)$), the package addressed

[2] Realizability has many more applications, for example in proof theory, where it can be used to show interesting properties of constructive systems that fail for their classical counterparts.

logical problems arising from the need to interpret the results of interval arithmetic differently in different situations. (For example, setting $\sqrt{([-1,4])}$ to $[0,2]$ during computation of an expression E leads to correct conclusions in some contexts, but can lead one to incorrectly conclude that a fixed point exists in the context of verifying the hypotheses of the Brouwer fixed point theorem.) These logical problems are addressed in IEEE-1788 with a *decoration system*, and there are several implementations. However, higher-level work utilising this system has not yet appeared in publications, and the decoration system remains somewhat controversial among implementers, primarily due to the extra work involved in implementation and to the question of efficiency.

In the mean time, interval arithmetic has been adopted by many outside the core of experts (numbering perhaps several hundred) on the subject. As an example of this, Goluskin has used the VSDP package [46] for obtaining rigorous upper and lower bounds on the solutions to semidefinite programs to ascertain bounds on average values in dynamical systems, such as average temperature in an atmospheric system [34].

Interval arithmetic has been particularly successful in supplying mathematical rigor to deterministic algorithms for global optimization of functions.

A continuing problem associated with interval arithmetic is that of overestimation: an interval evaluation $\mathbf{E}(\mathbf{x})$ of an expression E over the interval $\mathbf{x}$ always will contain the range $\{E(x) \mid x \in \mathbf{x}\}$, but the set difference

$$\mathbf{E}(\mathbf{x}) \setminus \{E(x) \mid x \in \mathbf{x}\}$$

may be so large that $\mathbf{E}(\mathbf{x})$ is useless for practical purposes; In other words, the lower and upper bounds on the range of E are, in general, not sufficiently sharp to be of use. Much research has focused on reducing this overestimation, and on identifying individual problems and types of problems in which this overestimation is not excessive. It has often occurred that rigorously bounded solutions to small, example problems can be found (and published), yet larger, more physically realistic models cannot, due to additional overestimation in the larger systems or to the computational cost of the alternative algorithms needed to avoid that overestimation. This has been particularly the case in the numerical solution of partial differential equation models (such as those of fluid dynamics), although inroads are constantly being made.

3 Presentation Highlights

3.1 Introductory Tutorials

There meeting began with four two-hour tutorial sessions introducing aspects of constructive analysis and interval arithmetic:

1. *Interval Arithmetic: Fundamentals, History, and Semantics* (presented by Baker Kearfott)
2. *Constructive Analysis: Philosophy, Proof, and Fundamentals* (presented by Hajime Ishihara)
3. *Verification Methods—mathematically correct results in floating-point* (presented by Siegfried Rump)
4. *Implementing Computable Analysis* (presented by Jens Blanck)

Kearfott began with the fundamentals of classical and interval arithmetic, emphasising its power to produce rigorously bounding roundoff error, and its theoretical and practical applications (for example, in Hales's proof of the Kepler Conjecture, and in collision avoidance in robotics). He then gave a comprehensive account of the history of interval arithmetic, before discussing logical pitfalls of the technique, and, finally, the IEEE Standard.

After a brief history of constructivism in mathematics, **Ishihara** explained the BHK-interpretation of the logical connectives and quantifiers, and intuitionistic natural deduction, followed by omniscience principles, constructive set theory (CZF) and choice axioms, number systems, apartness and equality, arithmetic and Cauchy- and order-completeness of $\mathbb{R}$. He ended with a discussion of the intermediate value theorem in the classical and constructive settings.

Rump provided details and examples on how a computer's floating-point arithmetic can be used to obtain mathematically rigorous results. He distinguished between discretisation of a continuous problem—such as replacing a system of partial differential equations (PDEs) with a system of nonlinear equations, and then finding mathematically rigorous bounds on solutions of the nonlinear equations—and finding mathematically rigorous solutions of the problem itself. He also presented his examples of where increasing the floating-point precision of a computation does not give insight into bounds on the actual solution. He gave details of the directed rounding and interval arithmetic mentioned by Kearfott in the first tutorial, then presented details of `Intlab`, discussing various algorithms common in interval computations. In the second part of his talk, he explained interval-arithmetic-based global optimization algorithms, illustrating the advantages with the Griewank function. He then continued with numerous details of interval-based techniques in global optimisation. Rump is in the process of developing a competitive global optimisation algorithm in `Intlab`.

Blanck's talk began with a brief outline of the connections, such as realizability, between constructive analysis, computable analysis, and interval arithmetic. He then discussed the problem of using finite information to compute approximations to countable objects, an approximation of an element $x \in X$ being 'a finite piece of information about x'. Introducing a natural partial order on approximations, he led us to Scott domains and their use as representations of topological spaces. He then dealt with approximations of reals, comparing rational approximations with interval ones and others, and with computing over spaces of functions and (compact) sets. The final part of his talk was devoted to implementation in Haskell.

3.2 Other talks

There were, strangely, no talks dealing with constructive analysis *per se*, although both Ishihara and Blanck discussed the intermediate value theorem in their tutorials.

There was one talk on constructive algebra, *Towards a constructive theory of O-minimal structures*, by Lombardi, in which he proposed a geometric theory for the algebra of real numbers, as 'a constructive rewriting of the classical theory of real closed rings'.

There were two talks on topology. Ciraulo began by explaining the fundamentals of Sambin's constructive point-free topology, and its relation to continuous domains and interval analysis. He then discussed positivity relations and localic sublattices, leading to a novel point-free perspective on interval numbers. Petrakis discussed his research in Bishop (function-) spaces, before introducing the notion of Comfort-compactness and showing its applicability—in particular, to a constructive Stone-Čech compactification theorem.

There were five talks presenting recent progress in program extraction. In the first of these, Spreen introduced, and then applied, the abstract notion of a digit space [13]. Using a (classically trivial) co-inductive definition, he constructively characterised those elements of compact Hausdorff space X that have a tree representation through their realizers. Taking X to be the hyperspace of compact subsets of a compact metric space equipped with the Hausdorff metric, he showed how to obtain tree representations of compact sets, representations that can be used, for example, for rendering such sets through program extraction.

Schwichtenberg showed how to represent an intensional version of Tsuiki's infinite Gray code through a simultaneous co-inductive definition, more precisely as the co-total elements of two simultaneously defined free algebras [12]. He gave constructive proofs of the equivalence of infinite Gray code and the signed digit representation of real numbers, and proved closure of the characterising co-inductive predicates under addition. From these proofs, formalised in the Minlog system, one can extract programs translating between the two representations as well as programs for addition on these representations. He stressed the crucial importance of certain refinements of the logic (non-computational quantifiers, uniform and non-uniform versions of logical operators) to obtain practically useful programs that do not contain junk [64].

Tsuiki described the partial and non-deterministic nature of infinite Gray-code and showed how to process it using an IM2-machine [77], a variant of a Turing machine. He compared the programs extracted from proofs (as described in Schwichtenberg's talk) with the corresponding IM2-programs and pointed out a certain mismatch, inherent in the different programming paradigms these programs are based on, to overcome which is still an open problem.

Berger presented an approach to capture bounded non-determinism logically through a modal operator S_n, generalising earlier work on unbounded non-determinism [8]. Realizers of a formula $S_n(A)$ are of the form $\mathrm{Amb}(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n$ are programs running in parallel, each trying to compute a realizer of A. Any terminating a_i counts as a possible result of the computation. Berger presented the logic for S_n and showed that one can extract programs that are close to Tsuiki's IM2-machines.

Bickford's talk dealt with the elder statesman of program extraction: the Nuprl project of Constable's group at Cornell. He presented the basic essence of Nuprl, before showing how, with recent extensions, the Cornell group has used it to prove both Brouwer's bar induction and a 'truncated version' of his continuity principle.

There were two talks on constructive reverse mathematics. Nemoto began by comparing the logical status of the intermediate value theorem (IVT) and the weak Konig lemma (WKL: every infinite binary tree has a path) in three foundational systems. Noting that although WKL implies IVT in those systems, the converse holds in only one of them, she showed how $\mathrm{WKL_c}$, the weak Konig lemma for convex trees, is equivalent, without countable choice, to IVT in an informal constructive foundation. Her proofs can be formalised over the system $\mathbf{EL}_0$.

Lubarsky's talk was on his (joint) work on topological models of constructive analysis, and in particular their application to separating different constructive notions of Cauchyness for sequences.

Benet described implementation of interval arithmetic in the Julia programming language for numerical analysis and scientific computing. (The Julia language and implementation are designed to combine the flexibility of interpretive languages such as Matlab and Octave with the speed of compiled languages such as C++ or Fortran.) He motivated the material with a challenging physical problem: to explain the behavior of a ring of Saturn. He then discussed general aspects of Julia, described its interval package and performance benchmarks, and gave several illustrations of its syntax and capabilities; he also described its use in constraint programming. He concluded with an example of Taylor's automatic generation and bounding of Taylor polynomials in mathematically rigorous integration of ordinary differential equations.

Sainudiin discussed applications of interval arithmetic in air traffic control and several other areas. He extended interval arithmetic to trees representing partitions of rectangles or hyperrectangles. (Such partitions are common in interval arithmetic applications, and constructing an arithmetic over the partitions themselves is a useful device.) He gave details of the tree arithmetic and its properties, and showed how it is used in various applications.

Melquiond described how interval arithmetic is used in the `COQ` semi-automated formal proof assistant. `COQ` is an extensive, well-established system developed by many logicians and computer scientists.

The final morning of the meeting was devoted to three talks somewhat separate from the ones already described. Sanders presented his work on the connection between nonstandard analysis and constructive analysis, in which the former in some sense subsumes the latter.

Visquaíno's talk dealt with his work on various aspects, theoretical and applied, of minimal logic: the ex falso rule and the law of excluded middle, infinitary geometric theories, well-ordering principles, and computability over algebraic structures.

Macintyre talked about Schanuel's conjecture in number theory, beginning with a history of the topic, then leading us through modern developments, including his own work with Wilkie, and culminating in recent work of Kirby and Zilber.

4 Scientific Progress

Extensive informal, after-hours, one-on-one discussions occurred internally within each of the two groups, an important activity since participants were geographically widely dispersed and such discussions would otherwise have been cumbersome. Similar group discussions between the interval analysis and constructive mathematics people also occurred during dinner, the lunch break, and between talks and sessions. All of these idea exchanges are proving valuable in stimulating and shaping individual researcher's work.

5 Benefits of the Meeting

The purpose of the workshop was to bring together researchers working in interval analysis and constructive mathematics, two fields with common roots and a large intersection of interests but virtually zero previous contact. The almost ideal environment in Oaxaca and the relaxed atmosphere of the workshop greatly facilitated contact between researchers in the two schools, which are now aware not only of the other school's existence but also of its aims, methods, and accomplishments

It has been remarked that interval mathematics can be viewed as applied constructive mathematics. While that may be a rather simplistic view, it is certainly the case that constructive mathematicians, especially those working on program extraction from proofs, stand to benefit considerably by contact with interval mathematicians, and that the latter are now aware of the research potential, in their own field, of constructive methods and the now considerable body of actual mathematics developed constructively. So, expecting that individual researchers will maintain contact, we believe that future collaboration across the group boundaries will bring considerable benefit all round.

References

[1] K. Aehlig, U. Berger, M. Hofmann, and H. Schwichtenberg, An arithmetic for non-size-increasing polynomial-time computation, Theor. Comput. Sci. **318** (2004), 3–27.

[2] P. Aczel and M. Rathjen, *Constructive Set Theory*, in preparation; http://www1.maths.leeds.ac.uk/~rathjen/book.pdf

[3] Agda, http://wiki.portal.chalmers.se/agda/

[4] R. Alps and D. Bridges, *Morse Set Theory as a Foundation for Constructive Mathematics*, in preparation.

[5] J. Berger, The weak König lemma and uniform continuity, J. Symb. Logic **73**(3) (2008), 933–939.

[6] J. Berger and D. Bridges, The anti-Specker property, a Heine-Borel property, and uniform continuity, Archive for Math. Logic **46**(7–8) (2008), 583–592.

[7] J. Berger and G. Svindland, Convexity and constructive infima, Arch. Math. Logic **55** (2016), 873–881.

[8] U. Berger. Extracting nondeterministic concurrent programs. In *Proc. 25th EACSL 2016*, to appear 2016.

[9] U. Berger, S. Berghofer, P. Letouzey, and H. Schwichtenberg, Program extraction from normalization proofs, Studia Logica **82**(2006), 27–51.

[10] U. Berger, A. Lawrence, F. Nordvall-Forsberg, and M. Seisenberger, Extracting verified decision procedures: Dpll and resolution, Logical Methods in Computer Science **11** (2015), 1–18.

[11] U. Berger, K. Miyamoto, H. Schwichtenberg, and M. Seisenberger, Minlog - a tool for program extraction for supporting algebra and coalgebra. In *Algebra and Coalgebra in Computer Science* (A. Corradini et el., eds), Lecture Notes in Computer Science **6859**, 393–399, Springer, 2011.

[12] U. Berger, K. Miyamoto, H. Schwichtenberg, and H. Tsuiki, Logic for Gray-code computation, accepted for *Proof 2013 Proceedings*, 2016.

[13] U. Berger and D. Spreen, A coinductive approach to computing with compact sets, J. Logic and Analysis, 2016, to appear.

[14] U. Berger, H. Schwichtenberg, and M. Seisenberger, The Warshall algorithm and Dickson's lemma: Two examples of realistic program extraction, J. Automated Reasoning **26**(2) (2001), 205–221.

[15] M. Bickford, Constructive analysis and experimental analysis using the Nuprl system proof assistant, Cornell University, March 2016; http://www.nuprl.org/KB/show.php?ID=750

[16] E. Bishop, *Foundations of Constructive Analysis*, McGraw-Hill, New York, 1967.

[17] E. Bishop and D. Bridges, *Constructive Analysis*, Grundlehren der math. Wissenschaften **279**, Springer, Heidelberg, 1985.

[18] J. Bochnak, M. Coste, and M-F. Roy, *Real algebraic geometry*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Series 3, **36**, Springer, Berlin, 1998.

[19] D. Bridges, Reflections on function spaces, Ann. Pure Applied Logic **163** (2012), 101–110; doi:10.1016/j.apal.2011.06.018.

[20] D. Bridges, Characterising weak-operator continuous linear functionals on $\mathcal{B}(H)$ constructively, Documenta Math. **16** (2011), 597–617.

[21] D. Bridges and H. Ishihara, Constructive closed range and open mapping theorems, Indag. Math. (N.S.) **11** (2000), 509-516.

[22] D. Bridges, H. Ishihara, and L. Vîţă, Computing infima on convex sets, with applications in Hilbert space, Proc. Amer. Math. Soc. **132**(9) (2004), 2723–2732.

[23] D. Bridges, H. Ishihara, B. Spitters, Locating the range of an operator with an adjoint, Proc. Koninklijke Nederlandse Akad. Wetenschappen (Indag. Math.) N.S., **11**(3) (2003), 1–8.

[24] D. Bridges and L. Vîţă, *Techniques of Constructive Analysis*, Springer New York, 2006.

[25] D. Bridges and L. Vîţă, *Apartness and Uniformity: A Constructive Development*, CiE series Theory and Applications of Computability, Springer, Heidelberg, 2011.

[26] R. Constable et al., *Implementing Mathematics with the Nuprl Proof Development System*, Prentice-Hall, New Jersey, 1986.

[27] The Coq Proof Assistant, http://coq.inria.fr

[28] M. Coste, An introduction to O-minimal Geometry, Dip. Mat. Univ. Pisa, Dottorato di Ricerca in Matematica, Istituti Editoriali e Poligrafici Internazionali, Pisa, 2000.

[29] T. Coquand and H. Lombardi, A logical approach to abstract algebra, Math. Structures Comp. Sci. **16** (2006), 885–900.

[30] M. Coste, T. Lajous-Loaeza, H. Lombardi, M-F. Roy, Generalized Budan-Fourier theorem and virtual roots, J. Complexity **21**(4) (2005), 479–486.

[31] M. Coste, H. Lombardi, and M-F. Roy, Dynamical method in algebra: effective Nullstellensätze, Ann. Pure Appl. Logic **111**(3) (2001), 203–256.

[32] L. van den Dries, Tame topology and o-minimal structures, London Math. Soc. Lecture Notes **248**, Cambridge University Press, Cambridge, 1998.

[33] K. Gödel, Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes, Dialectica **12** (1958), 280–287.

[34] D. Goluskin, Bounding averages rigorously using semidefinite programming: Mean moments of the Lorenz system. Technical report, University of Michigan, 2016; https://arxiv.org/abs/1610.05335

[35] L. González-Vega, H. Lombardi, and L. Mahé, Virtual roots of real polynomials, J. Pure Appl. Algebra **124**(1–3) (1998), 147–166.

[36] T. Hales, A proof of the Kepler conjecture, Annals of Mathematics **162**(3) (2005), 1065–1185.

[37] H. Lombardi and C. Quitté, *Commutative algebra: constructive methods. Finite projective modules*, Algebra and Applications **20**, Springer, Dordrecht, 2015.

[38] IIEEE Standard for Floating-Point Arithmetic, IEEE, New York, NY, August 2008; http://dx.doi.org/10.1109/ieeestd.2008.4610935

[39] IEEE1788-2015—IEEE Standard for Interval Arithmetic, IEEE, New York, NY, June 2015; http://ieeexplore.ieee.org/servlet/opac?punumber=7140719

[40] H. Ishihara, Locating subsets of a Hilbert space, Proc. Amer. Math. Soc. **129** (2001), 1385-1390.

[41] H. Ishihara, Constructive reverse mathematics: compactness properties. In: *From Sets and Types to Topology and Analysis: Towards Practicable Foundations for Constructive Mathematics* (L. Crosilla and P. Schuster eds), Oxford University Press, 245-267, 2005.

[42] H. Ishihara, Reverse mathematics in Bishop's constructive mathematics, Phil. Scientiae, Cahier special **6** (2006), 43-59.

[43] H. Ishihara, Neighbourhood and quasi-apartness spaces, and separation properties, Proc. 3rd Workshop on Formal Topology, Padova, Italy, May 7-12, 2007.

[44] H. Ishihara, R. Mines, P. Schuster, L. Vîţă, Quasi-apartness and neighbourhood spaces, Ann. Pure Appl. Logic **141** (2006), 296-306.

[45] H. Ishihara and L. Vîţă, Locating subsets of a normed space, Proc. Amer. Math. Soc. **131** (2003), 3211-3220.

[46] C. Jansson, Vsdp: A matlab software package for verified semidefinite programming. In *Conference paper of NOLTA 2006,* 327330, 2006; http://www.ti3.tu-harburg. de/paper/jansson/Nolta06.pdf

[47] S. Kleene, Countable functionals. In *Constructivity in Mathematics* (A. Heyting ed.) 81–100. North-Holland, 1959.

[48] U. Kohlenbach, Effective bounds from ineffective proofs in analysis: an application of functional interpretation and majorization, J. Symbolic Logic **57** (1992**)**, 1239–1273.

[49] G. Kreisel, Interpretation of analysis by means of constructive functionals of finite types. In *Constructivity in Mathematics* (A. Heyting, ed.), 101–128. North-Holland, 1959.

[50] A. Lawrence, U. Berger, and M. Seisenberger, Extracting a dpll algorithm, Electr. Notes in Theor. Comp. Sci. **286 (**2012), 243–256.

[51] I. Loeb, Equivalents of the (weak) fan theorem, Ann. Pure Applied Logic **132** (2005), 51–66.

[52] H. Lombardi, D. Perrucci, and M-F. Roy, An elementary recursive bound for effective Positivstellensatz and Hilbert 17th problem, Preprint, 2014; http://arxiv.org/abs/1404.2338

[53] H. Lombardi and C. Quitté, *Commutative algebra: constructive methods. Finite projective modules*, Algebra and Applications **20**, Springer, Dordrecht, 2015.

[54] The Minlog System, http://www.mathematik.uni-muenchen.de/$\sim$minlog/

[55] P. Martin-Löf, An intuitionistic theory of types. In *Twenty-five years of constructive type theory* (G. Sambin and J. Smith, eds), Oxford Logic Guides **36**, 83–111, Oxford University Press, 1998.

[56] R. Mines, F. Richman,and W. Ruitenburg, *A course in constructive algebra*, Universitext, Springer, New York, 1988.

[57] R. Moore, *Interval Arithmetic and Automatic Error Analysis in Digital Computing,* Dissertation, Department of Mathematics, Stanford University, 1962.

[58] R. Moore, R.B. Kearfott, and M. Cloud, *Introduction to interval analysis*, SIAM, Philadelphia, PA, USA, 2009.

[59] I. Petrakis, *Constructive Topology of Bishop Spaces* , Dissertation Univ. München, Fakultät für Mathematik, Informatik und Statistik, 2015.

[60] S.A. Naimpally and B.D. Warrack, *Proximity Spaces,* Cambridge Tracts in Math. and Math. Physics, Cambridge Univ. Press, Cambridge, U.K., 1979.

[61] I. Petrakis, The Urysohn Extension Theorem for Bishop Spaces. In *Symposium on Logical Foundations in Computer Science 2016* (S. Artemov and A. Nerode, eds), Lecture Notes in Computer Science **9537**, 299-316, Springer, 2016; doi: 10.1007/978-3-319-27683-0-21

[62] I. Petrakis, A direct constructive proof of a Stone-Weierstrass theorem for metric spaces. In *Pursuit of the Universal, CiE 2016* (A. Beckmann, L. Bienvenu and N. Jonoska, eds), Lecture Notes in Computer Science **9709,** 364-374, Springer, 2016; doi: 10.1007/978-3-319-40189-8-37

[63] A. Prestel, and N. Schwartz, Model theory of real closed rings. In *Valuation theory and its applications* (Vol. I) (F-V. Kuhlmann et al., eds), Fields Inst. Commun. **32**, 261–290, Saskatoon, SK, 1999; Amer. Math. Soc., Providence, RI, 2002.

[64] D. Ratiu and H. Schwichtenberg, Decorating proofs. In *Proofs, Categories and Computations—Essays in Honor of Grigori Mints* (S. Feferman and W. Sieg, eds), 171–188, College Publications, 2010.

[65] F. Richman, The constructive theory of countable abelian p-groups, Pac. J. Math. **45** (1973), 621–637.

[66] F. Richman, Constructive aspects of Noetherian rings, Proc. Amer. Math. Soc. **44** (1974), 436-441.

[67] F. Richman, Adjoints and the image of the ball, Proc. Amer. Math. Soc. **129** (2001), 1189–1193.

[68] F. Richman, The fundamental theorem of algebra: a constructive development without choice, Pacific J. Math. **196**(1) (2000), 213–230.

[69] S. Rump, INTLAB–INTerval LABoratory. In *Developments in Reliable Computing (*T. Csendes, ed.), Volume 5(3) of *Reliable Computing = Nadezhnye vychisleniia*, 77–104, Kluwer Academic Publishers Group; http://www.ti3.tu-harburg.de/rump/intlab/

[70] G. Sambin, Intuitionistic Formal Spaces—A First Communication. In *Mathematical Logic and its Applications* (D. Skordev, ed.), 187–204, Plenum Press, New York and London, 1987.

[71] G. Sambin, Some points in formal topology, Theoretical Computer Science 305 (2003), 347-408.

[72] G. Sambin, *Positive Topology and the Basic Picture. New structures emerging from Constructive Mathematics*, Oxford Logic Guides, Oxford University Press, to appear, 2018.

[73] H. Schwichtenberg, M. Seisenberger, and F. Wiesnet, Higman's lemma and its computational content. In *Advances in Proof Theory* (R. Kahle et al., eds), Progress in Computer Science and Applied Logic **28**, Springer International Publishing Switzerland, 2016; doi 10.1007/978-3-319-29198-7_11

[74] H. Schwichtenberg and S. Wainer, *Proofs and Computations*, Cambridge University Press, 2012.

[75] B. Spitters, Constructive Results on Operator Algebras, Journal of Universal Computer Science 11(12) (2005), 2096–2113.

[76] M. Tressl, Super real closed rings, J. Fund. Math. **194**(2) (2007), 121–177.

[77] H. Tsuiki, Real Number Computation through Gray Code Embedding, Theor. Comp. Sci. **284**(2) (2002), 467–485.

[78] W. Tucker, A rigorous ODE solver and Smale's 14th problem, Found. Comput.Math **24** (2002), 53–117.

[79] I. Yengui, Constructive commutative algebra, Lecture Notes in Mathematics **2138**, Springer, 2015.