構成的数学の体系と実践

吉田　聡

数学文献を読む会
2017年6月23日

目次

1. BHK解釈

BHK解釈

構成的数学は**BHK** (Brouwer-Heyting-Kolmogorov) 解釈の下で展開される数学

	$A \vee B$	$\exists x A$
通常の数学の解釈	$\neg A \wedge \neg$Bを仮定すると矛盾	$\forall x \neg A$を仮定すると矛盾
BHK解釈	AまたはBの判定手続きを明示できる	$A(c)$を満たすcを構成する手続きを明示できる

BHK解釈は通常の数学においても許容されるが、通常の数学は他の解釈も許容する。

構成的証明

- BHK解釈の下で許容される証明(構成的証明)はアルゴリズムと見なせるもののみ。
- つまり、構成的数学では、
  - 定理:仕様
  - 証明:仕様を実行するアルゴリズム

  と理解することができる。

BHK解釈の下での制限

- 通常の数学の論理的規則のうち、BHK解釈の下では許容されないものがある。

例:任意のプログラムPに対して、数列 $\{a_n^P\}$ を

$$a_n^P = \begin{cases} 1 & (P\text{は}n\text{ステップ目で停止}) \\ 0 & (\text{それ以外}) \end{cases}$$

によって定義するとき、以下の命題はBHK解釈の下では許容されない。

$$\forall P\left[\exists n\left(a_n^P = 1\right) \vee \forall n\left(a_n^P = 0\right)\right]$$

- 実際にBHK解釈の下でこの命題が成り立つとすると、任意のプログラムに対して停止性が判定できることになってしまう。
- このことから、次のLPO(the Limited Principle of Omniscience)は許容されない:

  任意の0-1列$\{a_n\}$に対して、
  $\exists n(a_n = 1)$または$\forall n(a_n = 0)$
- さらに、このことから

  排中律: 任意の命題Aに対して、$A \vee \neg A$

  はBHK解釈の下では許容されない。

BHK解釈の下で許容されない命題

Omniscience principles:

- LPO
- WLPO(the Weak Limited Principle of Omuniscience):任意の0-1列$\{a_n\}$に対して、
  $\forall n(a_n = 0)$または$\neg\forall n(a_n = 0)$
- LLPO(the Lesser Limited Principle of Omniscience):高々1つの項について1を取り、他の項は0を取る$\{a_n\}$に対して、
  $\forall n(a_{2n} = 0)$または$\forall n(a_{2n+1} = 0)$

- WLPOを許容しない理由:

$$a_n = \begin{cases} 0 & (2n+4\text{は2つの素数の和である}) \\ 1 & (\text{それ以外}) \end{cases}$$

この数列$\{a_n\}$について、$\forall n(a_n = 0)$であるとき、かつそのときのみ、以下が成り立つ。
Goldbach予想:
任意の4以上の偶数は2つの素数の和で表される

つまり、BHK解釈の下では、WLPOが成り立つとすると、Goldbch予想の成否が決定することになる。

- LLPOを許容しない理由:

$$a_n = \begin{cases} 1 & \left(\begin{array}{l}\pi\text{を十進展開したとき、} \\ \text{初めて3が100個続けて現れたときの} \\ \text{最初の位は第}n\text{位}\end{array}\right) \\ 0 & (\text{それ以外}) \end{cases}$$

BHK解釈の下では、LLPOが成り立つとすると、3が100個続けて現れるのが偶数の位からではないのか、または奇数の位からではないのかが分かってしまう。

2. Bishopの構成的解析学

Bishopの体系

- 構成的数学(constructive mathematics)はBHK解釈の下で展開される数学体系の総称
- 構成的数学の代表的な3つ体系:
  - E. Bishopの構成的解析学
  - L.I.J. Brouwerの直観主義数学 (intuitionistic mathematics)
  - A.A. Markov. Jrの学派の構成的帰納的数学 (constructive recursive mathematics)

- Bishopの構成的解析学の体系はErrett Bishop が１９６７年に著した “Foundations of Constructive Analysis” において展開されている解析学の理論が基になっている。
- その後, その追随者がBishopの数学観を拡張および発展させる形で、実際の数学理論を展開した。
  - D. Bridges “*Constructive Functional Analysis*” (1979)
  - R. Mines, F. Richiman et al “Constructive Algebra” (1988)
  - D. Bridges and F. Richiman “*Vrieties of Constructive Mathematics*” (1987)
- また、Bishiopの体系の形式化もその後行われた。
  - J. Myhill “Constructive Set Theory” (1975)
  - M. Beeson “Foundations of Constructive Manthematics” (1985)

- Bishopの1976年の著書は長らく絶版になっていたが、2012年に復刻された。そこに、E. Beesonによる序文が新たに追加されている。
- BeesonによるBishopの構成的解析学の解説
  - Bishopの体系は通常の数学では明示されない手続きの明示するもの
    ⇒存在定理や判定定理に対して、実際に構成手続きや判定手続きを与えることができるか否かを明示する。
  - 通常の数学を否定し、新たな数学を与えることがBishopの目的ではない。**通常の数学にある構成的な部分と非構成的な部分を明示する体系を与える**ことが目的である。

- Bishopの体系に対する形式体系
  - $HA^{\omega} + AC_{00} + DC + AC!$
  - Martin-Loef’s type theory
  - constructive set theory

- Bishopの体系の特徴
  - BHK解釈に従う
  - fullの選択公理は許容しないが、制限された選択公理$AC_{00}, DC, AC!$を許容する。
  - Bishopの体系における定理は通常の数学の定理になっているが、その逆は成り立たない。
  - Omniscience principles は独立である（つまり、その肯定も否定も許容しない）。

Bishopの構成的解析学の定理

- 任意の実数a, b, cに対して、
  $a < b$ならば$a < c$または$c < b$.
  - Bishopの体系において
    $$\forall a, b \in \mathbf{R}[a \leq b \vee a > b] \leftrightarrow \mathrm{LPO}$$
    が証明可能。
- （**R**の完備性） 任意の実数値コーシー列は収束する
- （**R**の非可算性） 任意の実数列$\{x_n\}$に対して、すべてのnに対して$x_n \neq x$を満たす実数xが存在する

- （中間値の定理） fを区間$[a,b]$上の連続関数とし、$f(a)<0<f(b)$であるとする。このとき、任意の自然数kに対して、
$$|f(x)|<2^{-k} \text{ かつ } a<x<b$$
を満たす実数xが存在する。

- 次の命題はLLPOと同値：
fを区間$[a,b]$上の連続関数とし、$f(a)<0<f(b)$であるとする。このとき、$f(x)=0$ かつ $a<x<b$ を満たす実数 x が存在する。
- 関数を多項式関数や連続な単調増加（減少）に制限すれば、上記のよく知られた形も証明できる。

主な構成的数学の体系

- 直観主義数学
  - Bishopの体系 + WC-N + FAN
  - “すべての関数は連続関数”
  - LPO, WLPO, LLPOそれぞれの否定が成り立つ。
- 構成的帰納的数学
  - Bishopの体系 + CT_0 + MP
  - “すべての数学的対象は計算可能”
  - LPO, WLPO, LLPOの否定が成り立つ。

- 構成的数学の各体系に対する統一的な理解はそれらの形式体系が与えられたことで明らかになった。
- しかし、実際の数学の展開に関して、Bishop流、Brouwer流、Markov流のそれぞれで統一的に行われることなく、1990年頃まで基本的には個別に行われてきた。
  - Bishop流は通常の数学の部分系であるだけでなく、Brouwer流とMarkov流の部分系でもあるため、Bishop流の研究者は“Bishop流の研究＝構成的数学全体の研究”と述べていたこともある。
- 1980年代のM. Manderker および H. Ishiharaによる非構成的な命題 (omniscience principles)に関する研究から、それぞれの体系における数学の展開を統一的に行う枠組みが与えられた⇒**構成的逆数学**

計算可能数学

- 計算モデルに基づく計算可能な対象を定義。
  - 計算可能な実数、計算可能な関数など。
- 主要な体系
  - (Construtive recursive mathematics)
  - O. Averth “Computable analysis”(1980)
  - M. Pour-El and I. Richards “Computability in analysis and phisics”(1989)
  - K. Weihrauch “Computable analysis”(2000)
    - 近年、この体系における研究が盛ん。

Weihrauchの体系

- Type-2 Machine
  - 無限列の入出力を逐次実行するチューリングマシン。
  - 実数とその実数に収束する有理数列を同一視する。
  - Type-2 Machineによる実数の入出力は有理数列の逐次実行のこと。
- 「計算可能関数は連続である」
  - 対偶：与えられてた関数が連続でなければ計算可能でない
  - 実数値関数の連続性は適当なオラクルを持つType-2 Machineで計算可能性と同値であることを示している

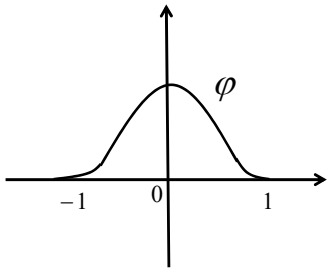
3.構成的数学の実践：Schwartz超関数の構成的理論

Schwartz超関数の構成的理論

$D(R)$: R上のテスト関数全体からなる位相ベクトル空間

- テスト関数の例：bump function φ

$$\varphi(x)=\begin{cases}\exp\left(-\dfrac{1}{1-x^2}\right) & (|x|<1, x\in I)\\ 0 & (|x|\geq 1, x\in I)\end{cases}$$



超関数： $D(\mathrm{R})$上の点列連続線形汎関数.

- 例： 任意のテスト関数φに対して、

$\langle \delta, \varphi \rangle := \delta(\varphi) := \varphi(0)$ （Diracのデルタ関数），

$\langle Y, \varphi \rangle = Y(\varphi) := \int_I \varphi(x)dx$（Heavisideの$Y$関数）.

区間I上で積分可能な関数fに対して、

$$\langle u_f, \varphi \rangle := \int_I f\varphi\, dx \qquad (\varphi \in D(R))$$

空間$D(\mathrm{R})$の完備化:$\widetilde{D}(R)$

- 通常の数学において、D(R)は完備性を持つ。
- Bishopの体系において、$D(R)$が完備であることの必要十分条件は命題BD-Nが成り立つこと(IY, 02)。
- 自然数からなる集合Aが次を満たすとき、pseudobounded であると言う:

任意のAの元からなる列$\{a_n\}$に対して、

$$a_n < n \quad (n \geq N)$$

を満たすNが存在する.

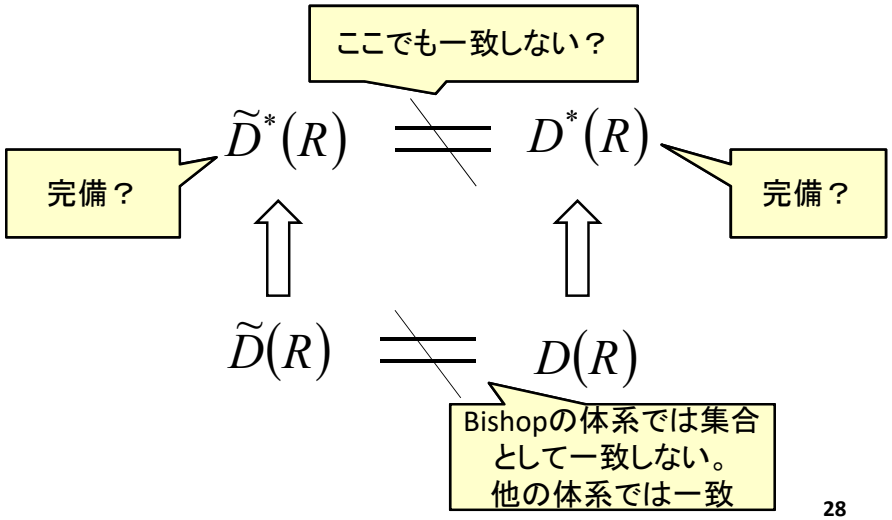
- 自然数からなる集合Aが上に有界でないとき、
  任意のnについて$a_n \geq n$ を満たすAの元からなる列$\{a_n\}$が存在する。
- この否定を考えたとき、pseduobounded の概念が現れる。
- 一方、次の命題はBishopの体系に対して独立である（Bridges, Ishihara et al. 2005):

BD-N: 任意の可算なpseudobounded な集合は有界

- つまり、Bishopの体系においては 有界性は pseudoboundedness を含意するものの、その逆は成り立たない。
- 一方、通常の数学、直観主義数学、構成的帰納的数学において、BD-Nは成り立つ(Ishihara 1992)。

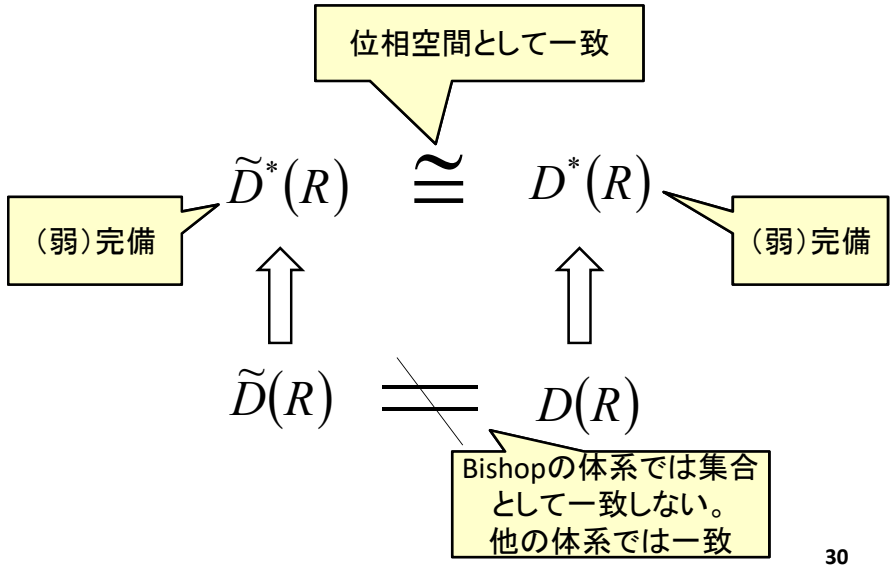
- $D(R)$ の完備性はBishopの体系では成立しない。
- そこで、$D(\mathrm{R})$のBishopの体系における完備化を与える。
  - テスト関数の条件を弱めることで得られる
  - 通常の数学において、$\widetilde{D}(R)$と$D(\mathrm{R})$は一致
- 双対空間 $D^*(R)$:超関数からなる空間
- 双対空間$\widetilde{D}^*(R)$:完備化$\widetilde{D}(R)$上の点列連続線形汎関数からなる空間
- 問題:
  1. $\widetilde{D}^*(R)$は(弱)完備か？
  2. $D^*(R)$は(弱)完備か？
  3. $D^*(R)$と$\widetilde{D}^*(R)$も一致しない？

空間$D(\mathrm{R})$の完備性と双対空間$D^*(\mathrm{R})$の弱完備性の問題



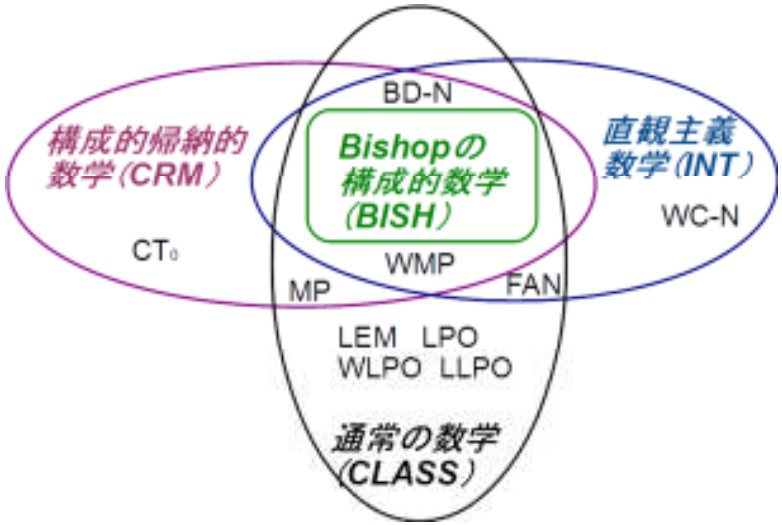
結果

1. $\tilde{D}^*(R)$は(弱)完備か？
   - 完備(Y, 03)。通常の数学と同様の証明。
2. $D^*(R)$は(弱)完備か？
   - 完備(Y, 03)
   - 通常の数学における多くの証明は$D(R)$の完備性を用いるが、本質的には必要ない。
3. $D^*(R)$と$\tilde{D}^*(R)$は一致しない？
   - 集合として一致。(Y,03)
   - 一方の空間の収束する列は一方の空間においても収束する(位相の一致)。(Y,13, preprint)



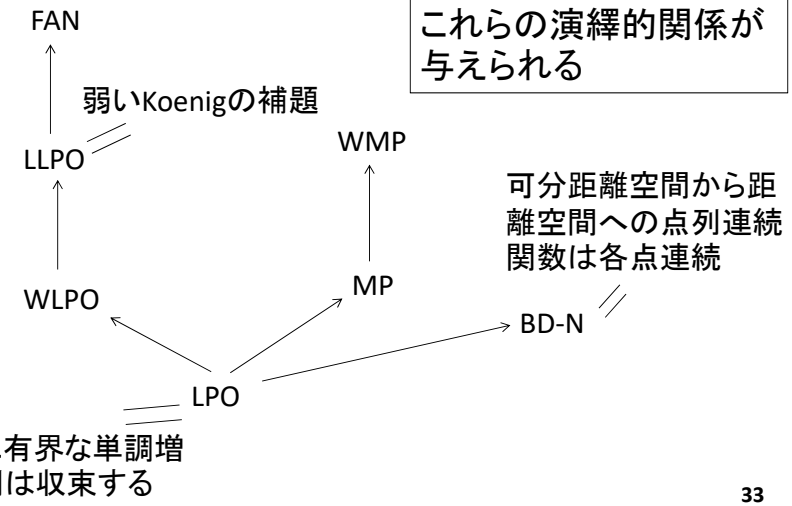
4.構成的数学の実践：構成的逆数学

各体系における定理の集合



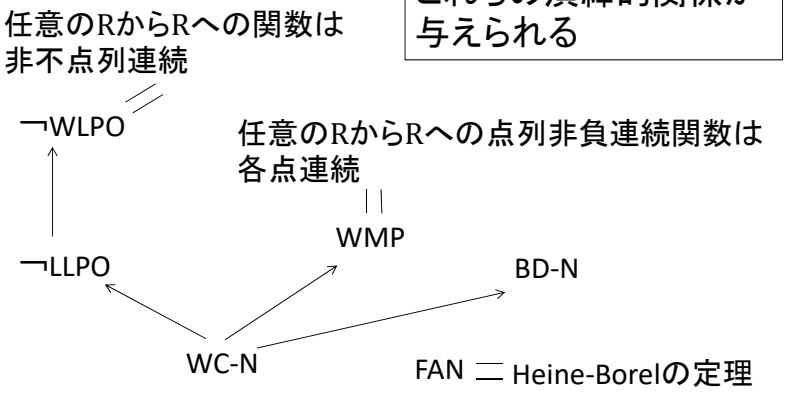
階層その1

Bishopの体系において、これらの演繹的関係が与えられる



階層その2（直観主義数学）

Bishopの体系において、これらの演繹的関係が与えられる



ただし、

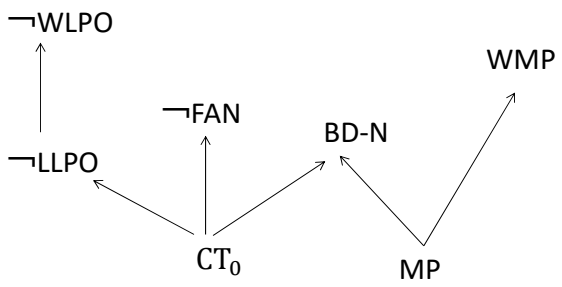
- $f \in R \to R$が次を満たすとき、**非不連続と呼ぶ**:

$$\forall\delta\forall\{a_n\}\forall a\left[a_n \to a\,(n\to\infty)\wedge\left|f(a_n)-f(a)\right|\geq\delta\Rightarrow\delta\leq 0\right]$$

- the Heine-Borelの定理:
  コンパクト空間の任意の被覆は有限部分被覆を持つ

階層その3（構成的帰納的数学）

Bishopの体系において、これらの演繹的関係が与えられる



- 構成的逆数学では、構成的数学の各体系の研究をBishopの体系をベースにして、必要に応じてOmniscience Principle　を仮定して理論を展開する。

- また、Bishopの体系をベースにした定理の論理的関係による分類が重要な研究テーマとなる　⇒通常の数学における**逆数学**との対比

5.構成的数学の実践：定理証明支援系によるシステム開発

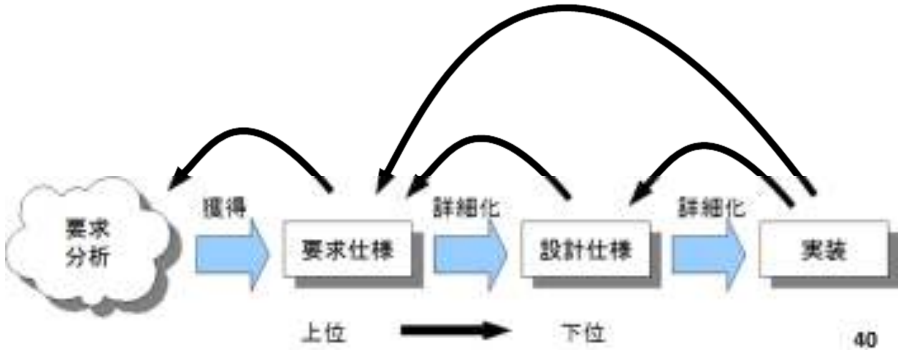
システム開発

- 要求仕様: 求める機能を述べたもの
- 設計仕様: 要求を実現するために行うことを述べたもの
  - 例：アルゴリズム
- 実装: 設計仕様を実行できる形で表現したもの
  - 例: プログラム

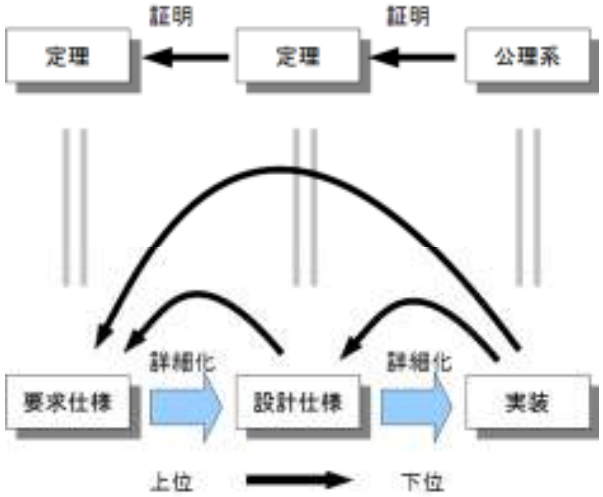
定理証明による検証

システムが正しく振舞うことの保証

- 下位のものが上位で述べていることを満たす振舞いをすることの証明、またはその根拠の提示



検証と数学理論との対応



- 定理証明支援系(proof assistant)
  - Coq: Calculus of (Inductive) Construction に基づく。INRIAなどにおいて開発。[参考文献 1]
  - Agda: Martin-Loef's type theory に基づく。Chalmers大学などにおいて開発。[参考文献 7]
- 構成的プログラミング
  - 構成的証明としてのプログラム開発。
  - 動作の正しさが保証されたプログラム
  - Coq, Agdaなどの定理証明支援系は構成的証明作成を支援する

定理証明支援系を含めた形式的手法(formal methods)を用いる意義

- IEC 61508
  - 電気・電子関連に関する機能安全規格
  - ソフトウェアに関して、SIL(safety integration level)の各レベル毎に推奨する開発手法がある。
  - 形式的手法はSIL2からSIL4において推奨されている
- ISO/IEC 15408(CC)
  - 情報技術を用いたシステムに関するセキュリティ規格

計算機科学と構成的数学

- 計算機科学
  - 処理を行う対象(データ構造)と主体(計算機、アルゴリズム)についての体系
- 構成的数学
  - 数学および数学的実践を担う主体についての体系
  - 数学的実践を担う主体:「手続きの明示」によってその主体は規定される

参考文献

1. R. Affeldt:定理証明支援系Coq入門, https://staff.aist.go.jp/reynald.affeldt/ssrcoq/coq-jssst2014.pdf, 2014.
2. H. Ishihara: Continuity properties in constructive mathematics, J. Symbolic Logic 57 (1992), 557-565.
3. H. Ishihara and S. Yoshida: A constructive look at the completeness of the space D(**R**), J. Symbolic Logic 67 (2002), 1511-1519.
4. U. Norell and J. Chapman: Dependently Typed Programming in Agda, 2008. http://www.cse.chalmers.se/~ulfn/papers/afp08/tutorial.pdf

参考文献

7. A. S. Troelstra and D. van Dalen: Constructivism in mathematics, vol. 1 and 2, North-Holland, Amsterdam, 1988.
8. S. Yoshida: The Banach-Steinhaus theorem for the space $D(\mathrm{R})$ in constructive analysis, Math. Logic Quart. 49(3), 305-315, 2003.
9. S. Yoshida: Generalized functions with pseudobounded support in constructive mathematics, J. Complexity 22(6), 783-802, 2006.
10. S: Yoshida: A note on the dual space of the constructive completion of the space $D(\mathrm{R})$, preprint, 2013.