Homotopy Probability Theory in the Univalent Foundations

Harry Crane

Department of Statistics
Rutgers

April 11, 2018

Motivating Comments/Questions

- First motivation: establish rigorous Foundation for Data Science/Statistics. (Will not discuss today.)

- Second motivation: consider whether a Foundation for mathematical practice can incorporate common intuitive/non-rigorous arguments ('without loss of generality', 'abuse of notation', conjecture).

  "A rigorous Foundation for non-rigorous math."

Example: Goldbach's conjecture

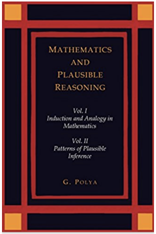
- No rigorous proof known.
- But can this be called a "rigorous conjecture"? (As of 2013: verified up to 4×10^{17}.)

Why should mathematicians care about non-rigor? (Part 1)

- Practicing mathematicians use 'non-rigorous' thinking all the time.

"We secure our mathematical knowledge by demonstrative reasoning*, but we support our conjectures by* plausible reasoning*.*

Demonstrative reasoning has rigid standards, codified and clarified by logic [...]. The standards of plausible reasoning are fluid, and there is no theory of such reasoning that could be compared to demonstrative logic in clarity or would command comparable consensus."
(Polyá, Mathematics and Plausible Reasoning*, 1954)*



Can there be a mathematical Foundation that treats conjectures as first-class mathematical objects (on par with theorems)?

Why should mathematicians care about non-rigor? (Part 2)

- Practicing mathematicians use 'non-rigorous' arguments all the time in 'rigorous' proofs.
- Example: Without Loss of Generality (WLOG)

Theorem

There are 6 total orderings of any set with 3 elements.

Proof: Without loss of generality let the set be $\{a, b, c\}$, then there are 6 orderings: $a < b < c$, $a < c < b$, $b < a < c$, $b < c < a$, $c < a < b$, and $c < b < a$. This exhausts all possibilities for $\{a, b, c\}$. The same argument carries over to any set with 3 elements, completing the proof.

Is this proof rigorous?

Why should mathematicians care about non-rigor? (Part 2)

Theorem

There are 6 bijections of a set with 3 elements.

Proof: Without loss of generality let the set be $\{a, b, c\}$, *then there are 6 orderings:* $a < b < c$, $a < c < b$, $b < a < c$, $b < c < a$, $c < a < b$, *and* $c < b < a$. *This exhaust all possibilities for* $\{a, b, c\}$. *By symmetry with any other set with 3-elements, this completes the proof.*

Barwise, 1989:

> *"[P]roofs where one establishes one of several cases and then observes that the others follow by symmetry considerations [constitute] a perfectly valid (and ubiquitous) form of mathematical reasoning, but I know of no system of formal deduction that admits of such a general rule."*

Awodey, 2014:

> *"This common practice is even sometimes referred to light-heartedly as "abuse of notation," [...] which is quite useful in practice, despite being literally false. It is, namely, incompatible with conventional foundations of mathematics in set theory."*

Why should mathematicians care about non-rigor? (Part 2)

Barwise, 1989:

> *"[P]roofs where one establishes one of several cases and then observes that the others follow by symmetry considerations [constitute] a perfectly valid (and ubiquitous) form of mathematical reasoning, but I know of no system of formal deduction that admits of such a general rule."*

Awodey, 2014:

> *"This common practice is even sometimes referred to light-heartedly as "abuse of notation," [...] which is quite useful in practice, despite being literally false. It is, namely, incompatible with conventional foundations of mathematics in set theory."*

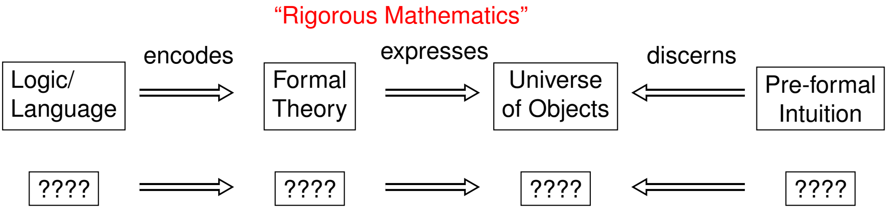
Can there be a mathematical Foundation under which standard forms of argument (e,g., WLOG) are logically valid?

H. Crane. (2018+). Without loss of generality, Univalent Foundations is a model of mathematical practice, and ZFC is not.

Outline

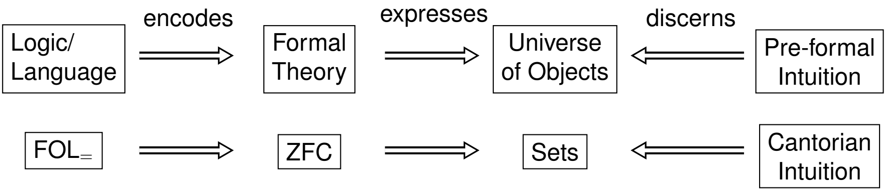
- Overview: The Big Picture
- Martin-Löf Type Theory (MLTT)
- Propositions-as-Types and Conjectures-as-Propositions in MLTT
- Homotopy Type Theory (HoTT) and Univalent Foundations (UF)
- Univalence Axiom
- Homotopy Probability Theory as a logic for mathematical conjecture

The Big Picture



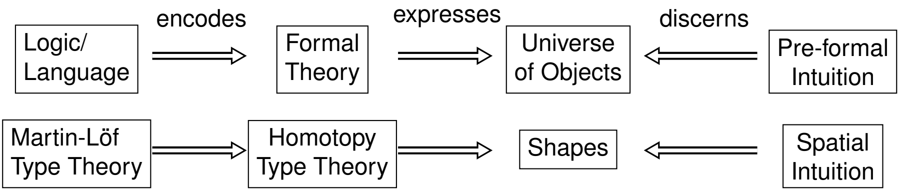
The Big Picture

“Rigorous Mathematics” (Set Theoretic Foundations)



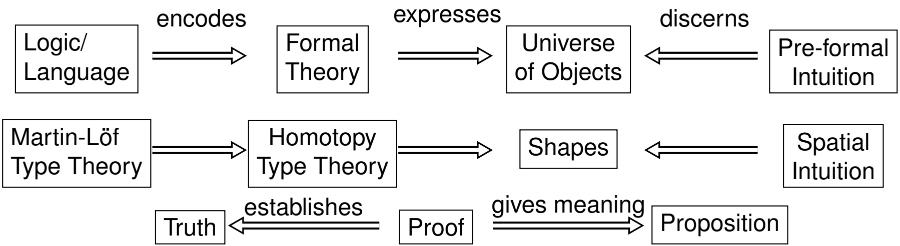
The Big Picture

“Rigorous Mathematics” (Univalent Foundations)



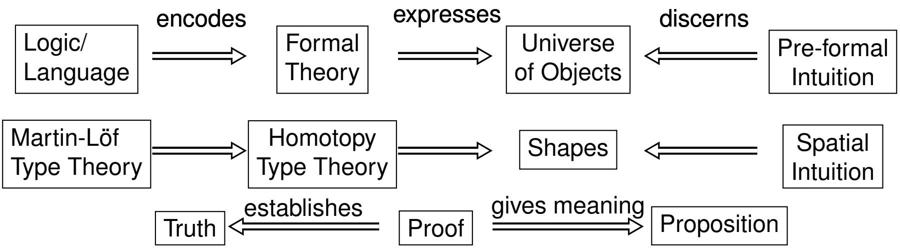
The Big Picture

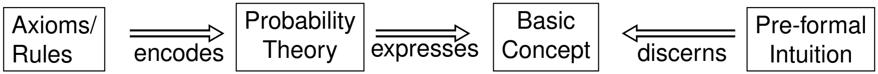
“Rigorous Mathematics” (Univalent Foundations)



The Big Picture

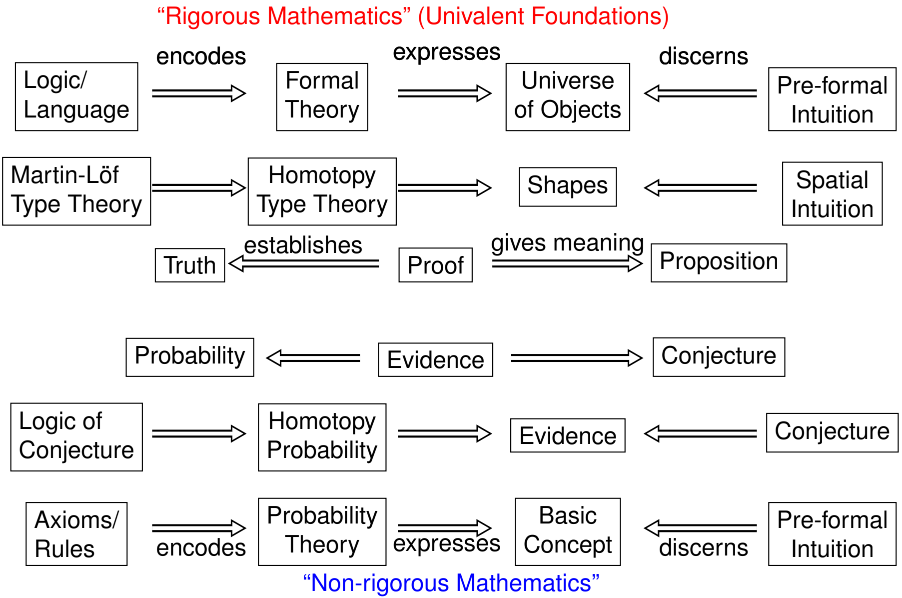
“Rigorous Mathematics” (Univalent Foundations)



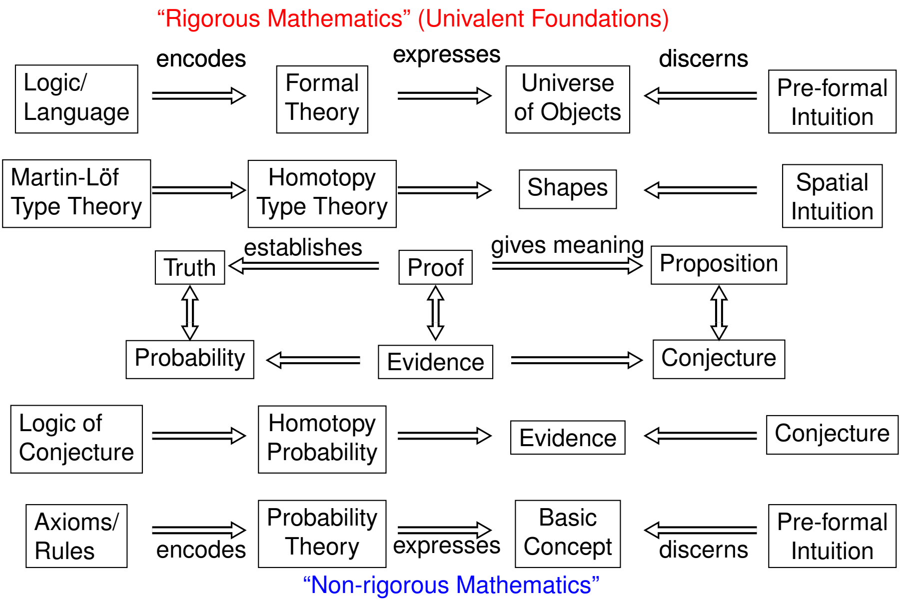


“Non-rigorous Mathematics”

The Big Picture



The Big Picture



Foundations of Probability

Axioms/ Rules	encodes ⟹	Probability Theory	expresses ⟹	Basic Concept	discerns ⟸	Pre-formal Intuition

Classical Probability (Mathematical)

Kolmogorov's Axioms	⟹	Frequentist Probability	⟹	Frequencies	⟸	Chance/ Randomness

Subjective/Bayesian Probability (Philosophical)

de Finetti's coherence	⟹	Subjective Probability	⟹	Prices of fair bets	⟸	Degrees of Belief

Homotopy Probability Theory (Logical)

Logic of Conjecture	⟹	Homotopy Probability	⟹	Evidence	⟸	Conjecture

Foundations of Probability

Axioms/ Rules $\Longrightarrow$ (encodes) Probability Theory $\Longrightarrow$ (expresses) Basic Concept $\Longleftarrow$ (discerns) Pre-formal Intuition

Classical Probability (Mathematical)

Kolmogorov's Axioms $\Longrightarrow$ Frequentist Probability $\Longrightarrow$ Frequencies $\Longleftarrow$ Chance/ Randomness

Interpretation

(K1) $\Pr(\Omega) = 1$
(K2) $\Pr(A) \geq 0$
(K3) Countable additive

A occurs with frequency $\Pr(A)$
Property A holds of proportion $\Pr(A)$ in collective

Example

Goldbach's Conjecture

Goldbach's conjecture has 99% probability to be true

Foundations of Probability

Axioms/ Rules $\Longrightarrow$ (encodes) Probability Theory $\Longrightarrow$ (expresses) Basic Concept $\Longleftarrow$ (discerns) Pre-formal Intuition

Subjective Probability (Philosophical)

de Finetti's coherence $\Longrightarrow$ Subjective Probability $\Longrightarrow$ Prices of fair bets $\Longleftarrow$ Degrees of Belief

Interpretation

(dF1) $\Pr(\Omega) = 1$
(dF2) $\Pr(A) \geq 0$
(dF3) Finite additive

Willingness to bet on A at odds $(1 - \Pr(A))/\Pr(A)$ or on $\neg A$ at $\Pr(A)/(1 - \Pr(A))$

Example

Goldbach's Conjecture

Willingness to bet at certain odds that Goldbach's conjecture is true

Foundations of Probability

Axioms/ Rules	encodes ⟹	Probability Theory	expresses ⟹	Basic Concept	discerns ⟸	Pre-formal Intuition
		Homotopy Probability		(Logical)		
Logic of Conjecture	⟹	Homotopy Probability	⟹	Evidence	⟸	Conjecture

Interpretation

Rules of inference for **Prob**(A) as a homotopy type in HoTT

Prob(A) is a 'body of evidence' supporting A.
Having a piece of evidence supports conjecture in A.

Example

Goldbach's Conjecture

Verifying first 4×10^{17} cases provides evidence to support Goldbach's conjecture.

Martin-Löf Type Theory (MLTT)

- Primitive objects: terms and types.
- Four primitive judgments:

judgment	meaning
A : **Type**	A is a type
$a : A$	a is a term of type A
$A \equiv A'$: **Type**	A and A' are identical types
$a \equiv a' : A$	a and a' are equal terms of A

- Possible interpretations:

a	A
term	type
element	set
proof	proposition
evidence	conjecture
algorithm	calculation
point	space

- **Key idea**: Propositions and Conjectures are mathematical objects, formalized as **types** in MLTT and later as **homotopy types** in homotopy type theory (HoTT).

Martin-Löf Type Theory (MLTT)

- Primitive objects: terms and types.
- Four primitive judgments:

judgment	meaning
A : **Type**	A is a type
$a : A$	a is a term of type A
$A \equiv A'$: **Type**	A and A' are identical types
$a \equiv a' : A$	a and a' are equal terms of A

- Possible interpretations:

a	A	
term	type	MLTT, syntax
element	set	ZFC, set theory
proof	**proposition**	**Curry–Howard, propositions-as-types**
evidence	**conjecture**	**C., Homotopy Probability Theory**
algorithm	calculation	Kolmogorov, Martin-Löf
point	space	HoTT

- **Key idea**: Propositions and Conjectures are mathematical objects, formalized as **types** in MLTT and later as **homotopy types** in homotopy type theory (HoTT).

Homotopy probability theory

- Proving a proposition (regarded as a type) amounts to constructing a proof (producing a term of the type).
- Propositions-as-types (Curry–Howard, 1959, 1969):

$$\text{term} : \text{type} \quad :: \quad \text{proof} : \text{proposition}$$

Can Curry–Howard be expanded to treat mathematical conjectures as first-class mathematical objects?

$$\begin{aligned} a &: A \\ \text{term} &: \text{type} \\ \text{proof} &: \text{proposition} \\ \text{evidence} &: \text{conjecture} \end{aligned}$$

Meta-mathematics for conjecture doesn't say what a conjecture is*, but rather what inferences are permissible based on conjectures.*

Syntax of MLTT

Proving a proposition $\iff$ *Constructing a term of an appropriate type*

Type theory	Interpretation (Curry–Howard)	Classical logic	Interpretation
A	proposition	A	proposition
$a : A$	a is a proof of A	$\vdash A$	A is true
$A \times B$	proof of both A and B	$A \wedge B$	A true and B true
$A + B$	proof of A or proof of B	$A \vee B$	A or B true
$A \to B$	proof of A implies proof of B	$\neg A \vee B$	if A then B
$\mathbf{0}$	empty type (contradiction)	$\perp$	false/contradiction
$A \to \mathbf{0}$	A implies contradiction	$\neg A$	not A
$\sum_{a:A} B(a)$	proof of $B(a)$ for some proof $a : A$	$\exists a\, B(a)$	exists a s.t. $B(a)$
$\prod_{a:A} B(a)$	proof of $B(a)$ for every proof $a : A$	$\forall a\, B(a)$	$B(a)$ for all a
$a =_A a'$	proof that a and a' identical	$x = y$	x and y are equal

Main differences:

- **Constructive**: Does not assume law of excluded middle ($A + \neg A$), but is consistent with it.
- **Computational**: Proving a proposition A requires computing a term of that type, $a : A$.
- **Proof relevance**: Different proofs are relevant to the calculus.
- **Identity type**: Distinct (but identical) proofs.

Proving a proposition $\iff$ *Constructing a term of an appropriate type*

MLTT	Curry–Howard	meaning
A	proposition	$a : A$ is a proof of A
$A \times B$	proof of A and proof of B	$(a, b) : A \times B$ for $a : A$ and $b : B$
$A + B$	proof of A or proof of B	$\mathtt{inl}(a) : A + B$ for $a : A$ or $\mathtt{inr}(b) : A + B$ for $b : B$
$A \to B$	proof of A implies proof of B	$g : A \to B$ converting $a : A$ to $g(a) : B$
$\mathbf{0}$	empty type	no terms of $\mathbf{0}$ (contradiction)
$A \to \mathbf{0}$	A implies contradiction	$g : A \to \mathbf{0}$ converts $a : A$ to $g(a) : \mathbf{0}$
	Dependent Types	
$\sum_{a:A} B(a)$	exists a s.t. $B(a)$	$(x, y) : \sum_{a:A} B(a)$ for $x : A$ and $y : B(x)$
$\prod_{a:A} B(a)$	$B(a)$ for all a	$f : \prod_{a:A} B(a)$ converts $a : A$ to $f(a) : B(a)$
	Identity Type	
$a =_A a'$	a and a' propositionally equal	$p : a =_A a'$ proof of identity

Example of a proof in MLTT

Theorem

For every proposition A, A implies $\neg\neg A$. In classical logic (with LEM), $A \leftrightarrow \neg\neg A$.

In syntax of MLTT,

$$(1) \quad \prod_{A:\mathbf{Type}} (A \to \neg\neg A) \qquad\qquad (2) \quad \prod_{A:\mathbf{Type}} (A + \neg A) \to (A \leftrightarrow \neg\neg A)$$

(1): *Given* $a : A$ *and* $g : \neg A \equiv A \to \mathbf{0}$, *derive* $g(a) : \mathbf{0}$. *Thus,* $\lambda a.\lambda g.g(a) : A \to \neg\neg A$.

(2): *Let* $\mathtt{LEM}_A : A + \neg A$. *The* $\to$ *direction follows from (1), without* $\mathtt{LEM}_A$. *The* $\leftarrow$ *direction follows since* $\mathtt{LEM}_A$ *implies either* A *or* $\neg A$ *holds and we construct* $A + \neg A \to (\neg\neg A \to A)$ *by case analysis.*

For $\mathtt{inl}(a) : A + \neg A$, *define* $\lambda g.a : \neg\neg A \to A$.

For $\mathtt{inr}(b) : A + \neg A$, *define* $\lambda g.\mathtt{efq}_A(g(b)) : \neg\neg A \to A$, *where* $\mathtt{efq}_A : \mathbf{0} \to A$.

We thus have a function $\Phi : A + \neg A \to (\neg\neg A \to A)$, *from which we derive* $\Phi(\mathtt{LEM}_A) : \neg\neg A \to A$, *completing the proof.*

(1) A conjecture of a proposition is itself a proposition:

$$\frac{A : \mathbf{Type}}{\mathbf{Conj}(A) : \mathbf{Type}} \quad \textit{(conj)}$$

(2) If a proposition has been proven, then there is evidence to support a conjecture:

$$\frac{A : \mathbf{Type} \qquad a : A}{\mathtt{evid}_A(a) : \mathbf{Conj}(A)} \quad \textit{(evid)}$$

(3) If A implies B, then a conjecture of A justifies a conjecture of B:

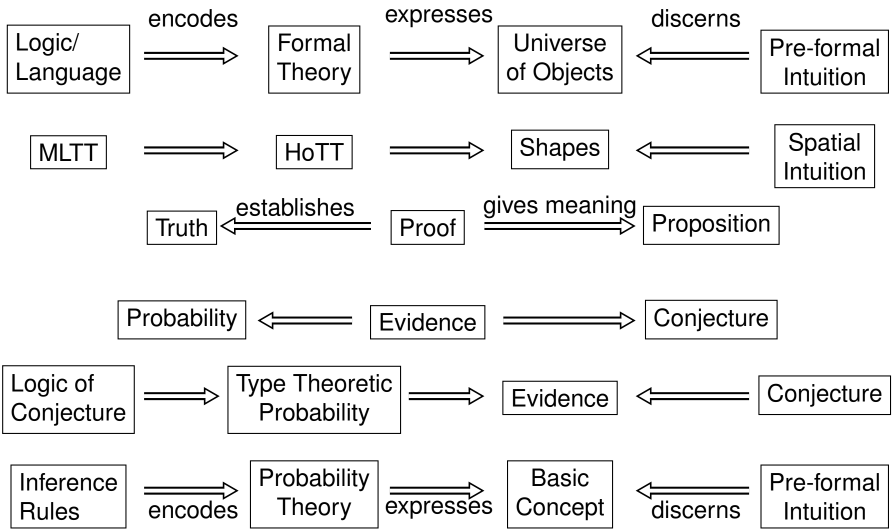
$$\frac{A : \mathbf{Type} \quad B : \mathbf{Type} \qquad f : A \to B}{\mathtt{imp}_{A,B}(f) : \mathbf{Conj}(A) \to \mathbf{Conj}(B)} \quad \textit{(imp)}$$

(4) Conjecturing a contradiction is a contradiction:

$$\frac{}{\mathbf{Conj}(\mathbf{0}) \equiv \mathbf{0} : \mathbf{Type}} \quad \textit{(conj-0)}$$

The Big Picture

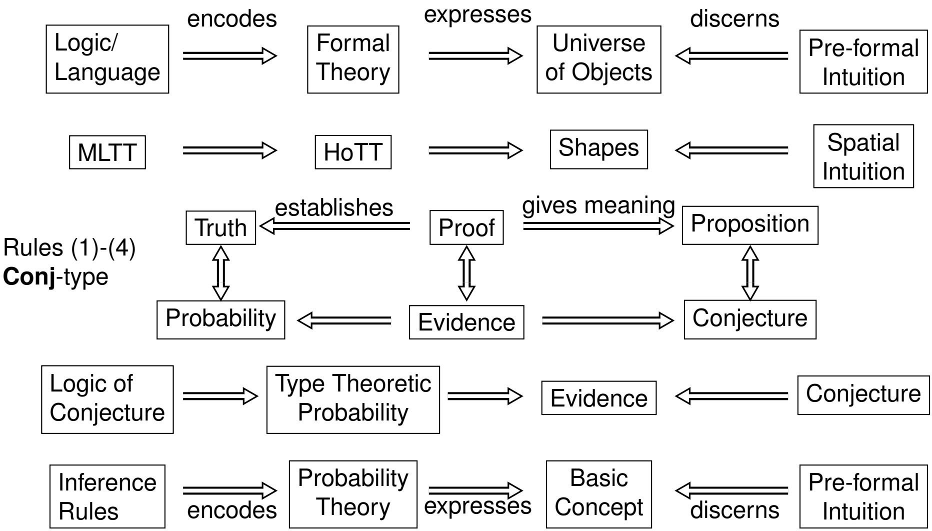
“Rigorous Mathematics” (Univalent Foundations)



“Non-rigorous Mathematics” (Type Theoretic Probability Theory)

The Big Picture

“Rigorous Mathematics” (Univalent Foundations)



“Non-rigorous Mathematics” (Type Theoretic Probability Theory)

Consequences of the Calculus for Conjecture

The following can be derived as **theorems** from the rules (1)-(4).

- $\prod_{a:\mathbf{Conj}(A)}\left(\left(\sum_{x:A}(\mathtt{evid}_A(x)=a)\to\mathbf{0}\right)\to\mathbf{0}\right)$

  Cannot rule out that evidence for a conjecture corresponds to a proof, but can't guarantee it either.

- Rules do **not** imply: $\prod_{a:\mathbf{Conj}(A)}\sum_{x:A}(\mathtt{evid}_A(x)=a)$.

  Calculus does not require that every conjecture is supported by proof.

- $\prod_{a:\mathbf{Conj}(A)}\mathbf{Conj}\left(\sum_{x:A}(\mathtt{evid}_A(x)=a)\right)$.

  A conjecture in A entails a conjecture that there is a proof of A consistent with that conjecture.

- $\mathbf{Conj}(A\times B)\to\mathbf{Conj}(A)\times\mathbf{Conj}(B)\to\mathbf{Conj}(A)+\mathbf{Conj}(B)\to\mathbf{Conj}(A+B)$

  Evidence for 'A and B' (jointly) implies evidence for A and evidence for B (individually), which in turn implies evidence for A or evidence for B, which implies evidence for 'A or B'. (Arrows do not reverse in general.)

Consequences of the Calculus for Conjecture

The following can be derived as **theorems** from the rules (1)-(4).

Universal/Existential quantification:

- $\mathbf{Conj}\left(\prod_{a:A} B(a)\right) \to \prod_{a:A} \mathbf{Conj}(B(a))$.

  Conjecturing that $B(a)$ holds for all $a : A$ entails a conjecture in $B(a)$ for every $a : A$.

- $\sum_{a:A} \mathbf{Conj}(B(a)) \to \mathbf{Conj}\left(\sum_{a:A} B(a)\right)$.

  Conjecturing $B(a)$ for some $a : A$ entails a conjecture that there exists $a : A$ such that $B(a)$ holds.

Derived inference rules:

- $\mathbf{Conj}(A) \times (A \to B) \to \mathbf{Conj}(A \times B)$

  Conjecturing A and having proof that A implies B entails a conjecture in A and B.

- $A \times \mathbf{Conj}(A \to B) \to \mathbf{Conj}(A \times B)$.

  Having proof of A and a conjecture that A implies B entails a conjecture in A and B.

Consequences of the Calculus of Conjecture

The following can be derived as **theorems** from the rules (1)-(4).

Higher-order conjectures:

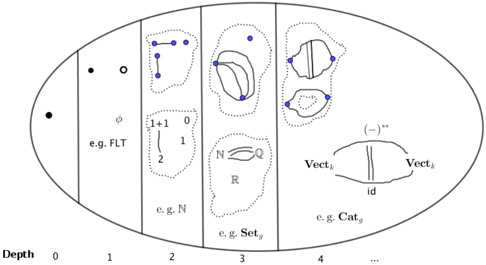
- Since **Conj**(A) is a type, iterate the **Conj** operator inductively:

$$\begin{aligned}\mathbf{Conj}_n(A) &: \mathbf{Type}\\ \mathbf{Conj}_0(A) &:\equiv A\\ \mathbf{Conj}_{n+1}(A) &:\equiv \mathbf{Conj}(\mathbf{Conj}_n(A)).\end{aligned}$$

- $\mathbf{Conj}_n(A) \times \mathbf{Conj}_m(A \to B) \to \mathbf{Conj}_{n+m}(A \times B)$

Homotopy Probability Theory (HPT)

- Interpret the conjecture type from MLTT into homotopy type theory (HoTT).
- A proposition is interpreted as a topological space (up to homotopy equivalence), with points given by proofs and paths between them.
- A conjecture is a topological space consisting of different pieces of evidence and the relations between them.
- Interpret **Type** as a universe $\mathcal{U}$ of homotopy types.



- **Homotopy type**: space up to continuous deformation.
- Propositional identity of terms formalized as a path between points.

Key Technical Addition: Univalence Axiom (Voevodsky)

$(A \simeq B)$	$\simeq$	$(A =_{\mathcal{U}} B)$
(homotopy) equivalence	*is equivalent to*	*identity*

- Homotopy equivalence: $A \simeq B$ is the homotopy type

$$A \simeq B :\equiv \sum_{f:A \to B} \left(\sum_{g:B \to A} (f \circ g \sim \mathtt{id}_B) \right) \times \left(\sum_{h:B \to A} (h \circ f \sim \mathtt{id}_A) \right) : \mathcal{U}.$$

- Two propositions (or conjectures) are identical if they can be continuously deformed one into the other. (Special case: isomorphism ($g = h = f^{-1}$).)
- Univalence Axiom: For all $A, B : \mathcal{U}$, there is an inhabitant of $(A \simeq B) \simeq (A =_{\mathcal{U}} B)$.
- Analog to Axiom of Extensionality (set theory): A and B are sets

$$(A = B) \leftrightarrow \forall x (x \in A \leftrightarrow x \in B).$$

- Practical consequence: if A and B are mere propositions (true or false), then

Univalence $\leftrightarrow$ Without Loss of Generality

$$\text{PropUA} \quad \leftrightarrow \quad \prod_{A:\text{Prop}_{\mathcal{U}}} \prod_{P:\text{Prop}_{\mathcal{U}} \to \text{Prop}_{\mathcal{U}}} \left(P(A) \to \prod_{B:\text{Prop}_{\mathcal{U}}} (A \simeq B) \to P(B) \right).$$

MLTT

- Type
- Term
- Equality
- Universal
- Existential
- Identity
- Universe

The Basic Notions of UF formalized in HoTT

MLTT	**Curry–Howard**
Type	Proposition
Term	Proof
Equality	Identification
Universal	For all
Existential	There exists
Identity	Logical Equivalence
Universe	Propositions

The Basic Notions of UF formalized in HoTT

MLTT	**Curry–Howard**	**HoTT**
Type	Proposition	Shape
Term	Proof	Point
Equality	Identification	Path
Universal	For all	Fiber (Map)
Existential	There exists	Total Shape
Identity	Logical Equivalence	Equivalence
Universe	Propositions	Universe

The Basic Notions of UF formalized in HoTT

MLTT	Curry–Howard	HoTT	Syntax (UF)
Type	Proposition	Shape	$X : \mathcal{U}$
Term	Proof	Point	$x : X$
Equality	Identification	Path	$p : a =_X b$
Universal	For all	Fiber (Map)	$\prod_{x:A} B(x) : \mathcal{U}$
Existential	There exists	Total Shape	$\sum_{x:A} B(x) : \mathcal{U}$
Identity	Logical Equivalence	Equivalence	$X \simeq Y$
Universe	Propositions	Universe	$\mathcal{U}$ with univalence

Homotopy Probability Theory in UF

With Univalence can express deeper notions about conjecture.

- **Independence of** A **and** B:

$$\mathbf{indep}(A, B) :\equiv (\mathbf{Conj}(A \times B) =_{\mathcal{U}} \mathbf{Conj}(A) \times \mathbf{Conj}(B)).$$

A and B are independent if conjecturing both A and B is equivalent to conjecturing each individually. (Evidence for A (resp. B) does not interfere with evidence for B (resp. A).)

- **Conditional conjecture of** B **given** $a : \mathbf{Conj}(A)$:

$$\mathbf{Conj}(B \mid a) :\equiv \sum_{x:\mathbf{Conj}(A \times B)} (\mathtt{imp}_{\mathtt{pr}_A}(x) = a).$$

Conditional conjecture in B given $a : \mathbf{Conj}(A)$ *is a conjecture x in A and B together with proof that x is compatible with a.*

Theorem (Law of Total Probability)

$\sum_{a:\mathbf{Conj}(A)} \mathbf{Conj}(B \mid a) \simeq \mathbf{Conj}(A \times B)$

Conjecturing A and B is equivalent to conjecturing A and then a conditional conjecture for B given the evidence favoring A.

With Univalence can express deeper notions about conjecture.

- **Independence of A and B:**

$$\mathbf{indep}(A, B) :\equiv (\mathbf{Conj}(A \times B) =_{\mathcal{U}} \mathbf{Conj}(A) \times \mathbf{Conj}(B)).$$

A and B are independent if conjecturing both A and B is equivalent to conjecturing each individually. (Evidence for A (resp. B) does not interfere with evidence for B (resp. A).)

- **Conditional conjecture of B given $a : \mathbf{Conj}(A)$:**

$$\mathbf{Conj}(B \mid a) :\equiv \sum_{x:\mathbf{Conj}(A\times B)} (\mathtt{imp}_{\mathtt{pr}_A}(x) = a).$$

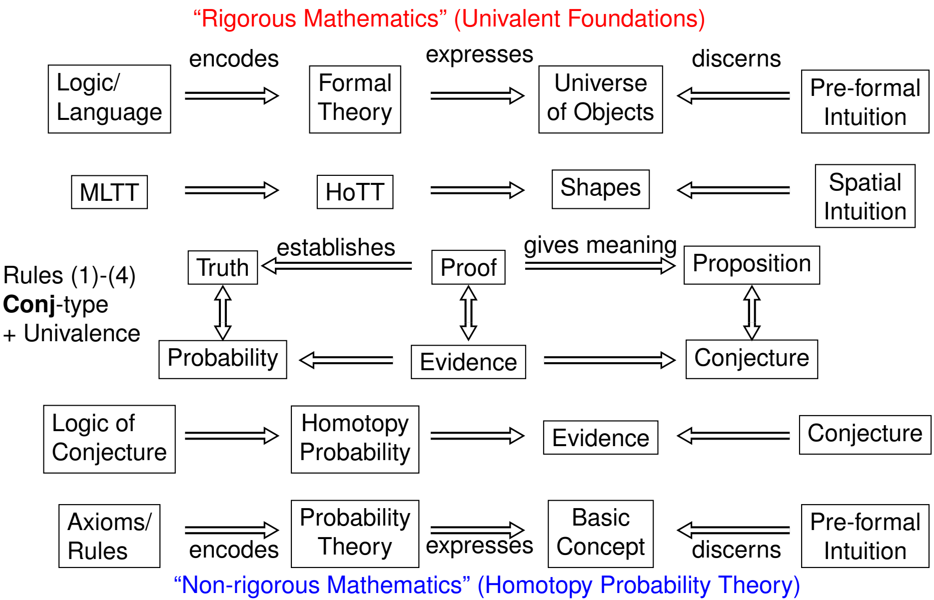
Conditional conjecture in B given $a : \mathbf{Conj}(A)$ is a conjecture x in A and B together with proof that x is compatible with a.

Theorem (Independence)

$$\mathbf{indep}(A, B) \simeq \left(\prod_{a:\mathbf{Conj}(A)} \mathbf{Conj}(B \mid a) \simeq \mathbf{Conj}(B)\right)$$

Independence of A and B is equivalent to independence of $\mathbf{Conj}(B \mid a)$ and a for all $a : \mathbf{Conj}(A)$.

The Big Picture



Summary: Homotopy Probability Theory in Univalent Foundations

Selling points	**Criticism**
Formalized math, computerized proof assistants (Coq, Agda).	Math is a human activity, no need for computers.
Richer than set theory (sets recovered as derived notion) $\Rightarrow$ can potentially encode much more structure.	UF introduces new, unfamiliar concepts. What more does it allow mathematician to do that cannot already do?
Univalence axiom faithful to the way mathematicians practice: equivalent objects are identical.	Univalence axiom is mysterious and unnatural. Sometimes isomorphic objects should be distinguished.
Univalence axiom is identical to WLOG (C. 2018+).	
Can incorporate conjecture in a rigorous meta-mathematical framework?	Why should mathematicians care about non-rigorous math?

References

- H. Crane. (2018). Logic of Probability and Conjecture. https://philpapers.org/rec/CRALOP
- H. Crane. (2018). Without loss of generality, Univalent Foundations is a model of mathematical practice, and ZFC is not.

- D. Tsementzis. (2017). First order logic with isomorphism. arXiv:1603.03092
- D. Tsementzis. (2017). A meaning explanation for HoTT. http://philsci-archive.pitt.edu/12824/1/A.Meaning.Explanation.for.HoTT.pdf

- The Univalent Foundations Program. (2013). *Homotopy Type Theory: The Univalent Foundations of Mathematics*.