(More details in https://www.cs.bu.edu/fac/lnd/.m/sta.pdf)

Set Theory in the Foundation of Math; Internal Classes, External Sets

Leonid A. Levin
www.cs.bu.edu/fac/Lnd

Boston University

BU, July 10, 2024

Set Theory in the Foundation of Math; Internal Classes, External Sets.
Outline

Set Theory: Some History, Self-Referentials
Dealing with the Concerns; Cardinalities
Going at the Self-Referential Root
Radical Computer Theorist Hits Back
Some Complexity Background
Independence Postulate
Reducing All Quantifiers to those on Integers
A Problem: One-Way Functions
Takeout: the Issues
Takeout: a Way to Handle
Some More **IP** Applications
Appendix: ZFC Axioms
To Modify ZFC

Set Theory: Some History, Self-Referentials

Cantor's Axioms: All Set Th. formulas define (quantifiable) sets.

In effect: formulas with quantifiers over formulas.
This self-referential aspect turned out fatal.

Zermelo, **F**raenkel: Restrict cardinality in Cantor's Axioms:
Replacement preserves it. A separate **Power Set** increases it.

Somewhat *ad-hoc* as foundations for math. And cardinality focus has questionable relevance. Distinctions between uncountable cardinalities almost never looked at in math papers.

Usual math sets have special types: countable, compact,
open, occasionally Borel, rarely projective, etc.
Generic subsets from Power Set classes, with no other descriptions, find little use in math and greatly complicate its foundations.

All consistent axiom systems have countable models. Cardinalities look like an artifact, designed to hide some self-referential aspects.

Dealing with the Concerns; Cardinalities

Logicians: Isolate math segments where more ingenious proofs can replace the use of Power Set Axiom and its uncountable sets.

Math folk: Bad to mess with math unity. Must keep whole its monumental structure ! And better not to complicate proofs.

Computer **T**heorist breaks in: Are there really any infinite objects?

Computer **T**(errorist): Timidity never works! Reject infinite sets.

Dear **C.T.:** Agreed about timidity, but drop your errorist aspect!

Infinities are neat: $\overline{\mathbb{R}}$ is compact, "less infinite" in that than $\mathbb{Q}$.

And handling (often ambiguous) termination points of objects is awkward. And 0, ∞ are great simplifying approximations to ϵ, $\frac{1}{\epsilon}$.

Going at the Self-Referential Root

Expanding Set Th. with more formula types, axioms, etc. has no natural end. Benefits little, eventual consistency loss inevitable.

ZF-restricted self-referentials, such as implicit quantifiers over formulas, brought no trouble so far, but find little math use either.

Let us try to drop any such excesses.

Externals: sets math handles (as values of variables, e.g., random strings), but does not internally specify. Mark them apart from **classes**: collections defined by math properties.

Math objects (only informally called sets) are classes $\{q\colon F_p(q)\}$ of sets q satisfying formulas F with external parameters p. Collections of objects are treated as collections of those parameters. Quantifiers bind parameters, not properties F.

Radical Computer Theorist Hits Back

Independence Postulate

Even with infinite complexities, external objects have finite information (small, really) about formula-defined classes.

Besides, it would be redundant for math objects F_p to duplicate in the external parameter p their formula-defined information.

Complexity theory allows to formalize that, justify the validity for "external data", and use that for simplifying math foundations.

This gives a way to handle infinitely complex sets, but reduce their quantifiers to those on **integers**. All with no seeming need to change anything in math papers, only reinterpret some formalities.

(In some cases one can state meta-theorems: a family with formula parameter F, as done now by Category Theorists.)

Some Complexity Background

Length $\|t\| \overset{\text{df}}{=} n$ for $t{\in}\{0,1\}^n$; $\|t\| \overset{\text{df}}{=} \lceil \log_2 t \rceil{-}1$ for $t{\in}\overline{\mathbb{R}^+}$.
The uniform on $\mathbf{\Omega} \overset{\text{df}}{=} \{0,1\}^{\mathbb{N}}$ distribution $\lambda(t\,\mathbf{\Omega}) \overset{\text{df}}{=} 2^{-\|t\|}$.

C.e. (computably enumerable) sets are ranges of algorithms.
C.e. function to $\overline{\mathbb{R}^+}$ is sup of a c.e. set of (continuous) basic ones.
C.e. $f{\in}D$ **dominates** Banach space D if all c.e. $g{\in}D$ are $O(f)$.

The λ-**test** is $\mathbf{d}(\alpha) \overset{\text{df}}{=} \|\lceil \mathbf{T}(\alpha) \rceil\|$ for c.e. $\mathbf{T}$: $\mathbf{\Omega}{\to}\overline{\mathbb{R}^+}$, $\lambda(\mathbf{T}){\leq}1$ that dominates $\mathbf{L}^1(\mathbf{\Omega}, \lambda)$. $\mathbf{M}(x) \overset{\text{df}}{=} \lambda(u^{-1}(x\,\mathbf{\Omega}))$ (u - universal alg.) is dominant among semimeasures $\{\mu : \forall x\ \mu(x) \geq \mu(x0){+}\mu(x1)\}$.

Kolmogorov–Martin-Lof λ-**randomness:** $\mathbf{R}^\lambda_c \overset{\text{df}}{=} \{\alpha : \mathbf{d}(\alpha){<}c\}$.
In terms of $\mathbf{M}$: $\mathbf{R}^\lambda \overset{\text{df}}{=} \mathbf{R}^\lambda_\infty = \{\alpha : \sup_{x \sqsubset \alpha}(\mathbf{M}(x)/\lambda(x\,\mathbf{\Omega})) < \infty\}$.

Mutual **Information:** $\mathbf{I}(\alpha_1{:}\alpha_2) \overset{\text{df}}{=} \min_{\beta_1,\beta_2}\{\mathbf{d}(\beta_1, \beta_2) : u(\beta_i){=}\alpha_i\}$.

Independence Postulate

$$\textbf{IP:} \quad \boxed{\forall\alpha\ \mathbf{I}(\alpha{:}\ F) < \infty}$$

(A family of axioms, one for each property $F \in \Delta^0_* \overset{\text{df}}{=} \cup_n \Delta^0_n \subset \mathbf{\Omega}$.)

(By **IP**, classes $\alpha{\in}\Delta^0_*$ double as sets only if computable.)

Justifications and Applications

Conservation laws: no processing of α, algorithmic, or random, or mixed, increases $\mathbf{I}(\alpha{:}F){+}O(1)$. Arguably, no physical process can.

Little expressive power loss: Any object F_α is also $\overline{F}_\beta$, $\mathbf{I}(\beta{:}\ G){<}\infty$: Any α has such β, each computable from the other and $G, 0'$.

If time allows, I can mention more, not ST, powerful applications.

Reducing All Quantifiers to those on Integers

IP opens a way: excludes $\alpha \in F_\beta$ unless such α reduce to a positive fraction of $u^{-1}(\beta)$. (Note: $\lambda(A|B){>}t$ has only integer quantifiers.)

But what about the reverse?

Primal Chaos axiom (**P**$\mathcal{X}$): "Each α reduces to even-indexed digits of some K-ML random $\beta \in \mathbf{R}^\lambda$."
(For classes, i.e. in ZF, it is the famous Gacs-Kucera theorem.)

A **model** (countable, in ZFC): Take a $\gamma{\in}\,\mathbf{\Omega}$, outside all $X{\in}\Delta^0_*$ of $\lambda(X){=}0$. Let $\gamma^{(k)} : i \mapsto (i \bmod k)\,\gamma_i$. γ-model includes all sets with "$\in$" on transitive closures enumerable from $\gamma^{(k)}$ for some k.

The model eliminates 2nd order quantifiers, obeying a c.e. family of axioms: $F \Leftrightarrow \lambda(\{\gamma\colon F^*(\gamma)\}) > 0$, where F^* has all real variables α_i in a sentence F replaced by $A_i(\gamma^{(k_i)})$; A_i, k_i quantified as integers.

A Problem: One-Way Functions

Extending **IP** with such a c.e. family of axioms does not strike me as really elegant and intuitive. I hoped, adding a single Gacs-Kucera Theorem as a fundamental Set Theory axiom would suffice.
(Hint: by **IP**, $\exists\alpha P(\alpha,\overline{\beta}) \Rightarrow \lambda(\{\gamma\colon \exists f\ P(f(\gamma),\overline{\beta})\} \mid u(\gamma){=}\overline{\beta}) > 0)$.
But deriving "$\Leftarrow$" via $\mathbf{P}\boldsymbol{\chi}$ meets an obstacle:

Recursively One-Way Functions on $S, \lambda(S){>}0$.
Let $\lambda(f^{-1}(x\,\boldsymbol{\Omega})\cap S) = O(\lambda(x\,\boldsymbol{\Omega}))$. f is **OW** on S if no g inverts it (f, g computable): $\lambda^2(\{(\beta,\gamma) : \alpha \overset{\text{df}}{=} g(\beta,\gamma){\in}S,\ f(\alpha){=}\beta\}) = 0$.
They do exist: [Barmpalias, Gacs, Zhang: 2024].

Handling OWFs demands more tools. A single axiom would be more elegant and intuitive than the whole c.e. family from the above model. I have some ideas but the problem is still open.

Takeout: the Issues

1. Cardinality-based ZF restrictions of Cantor's Axiom defuse self-referential problems but do not eliminate their source. A bit *ad-hoc*, and result in a Babel Tower of cardinalities, other hierarchies, that find little relevance in math.

2. Replacing Power Set in segments of math with more elaborate proofs (as Reverse Math, some others do) breaks the unity of math, so does not seem to be the right solution.

3. I blame the blurred distinction between internal (math-defined) and external (the domain of variables) aspects of math objects.

4. Extending Set Theory reach has no limits. Including in quantifiable domains formulas or classes they define just climbs higher in that direction. Little relevance to mainstream math.

Takeout: a Way to Handle

5. Separating formulas F from external variables values p in math objects F_p allows restricting formula-related information from p.

6. Complexity theory allows to formalize that, justify the validity for "external data", and use that for simplifying math foundations.

7. What is left out? – "Logical" sets, related to infinite hierarchies of formulas, such as "The set of all true sentences of Arithmetic".
Those should be subject of math **foundations**.
Theories cannot include their own foundations.

IP has a number of impressive (to myself at least) applications.
But I am against holding hostages for long.
So I will mention a couple and let you be free.

Some More **IP** Applications

Foundations of Probability Theory. Paradoxes in its application led to the concept of K-ML Randomness $\mathbf{R}^\lambda$. **IP** clarifies its use: For any $S\subset \mathbf{\Omega}$: $\lambda(S)=0$ if and only if $\exists\sigma\ S\cap\mathbf{R}^\lambda \subset \{\gamma : \mathbf{I}(\gamma{:}\sigma)=\infty\}$.

Goedel Theorem Loophole. Goedel writes:

> *"It is not at all excluded by the negative results mentioned earlier that nevertheless every clearly posed mathematical yes-or-no question is solvable in this way. For it is just this becoming evident of more and more new axioms on the basis of the meaning of the primitive notions that a machine cannot imitate."*

No way ! Let a predicate P on $\{0,1\}^n$ extend "proven/refuted" partial predicate of Peano Arithmetic. Let r_n be the n-bit prefix of a c.e. real $r = \min \mathbf{R}^\lambda_0$. Then $\mathbf{I}(P : r_n) = n \pm O(\log n)$.

Appendix: ZFC Axioms

1. **Membership chains: sources, sinks**. (1b anti-dual to 1a) :

1a. Infinity (a set with no source): $\boxed{\exists S, s\in S\,\forall x\in S\,\exists y\in S(x\in y)}$

1b. Foundation (sink in any set): $\boxed{\neg\exists S, s\in S\,\forall x\in S\,\exists y\in S(y\in x)}$

2. **Formula-defined Sets** ($R_c(X)\overset{\text{df}}{=}\{y : \exists x\in X\ R_c(x,y)\}$) :

2a. Extensionality (content identifies sets): $\boxed{x\supset y\supset x\in t \Rightarrow y\in t}$

2b. Replacement: $\boxed{(\forall x\,\exists Y\supset R_c(\{x\})) \Rightarrow \forall X\,\exists Y\supset R_c(X)\supset Y}$

3. **Function Inverses** $f^{-1}\overset{\text{df}}{=}\{g : f(g(x))=x,\ \mathrm{Dom}(g)=\mathrm{Im}(f)\}$:

3a. Powerset (f^{-1} is a set: $h=f^{T}$): $\boxed{\forall h\exists G\,\forall g\,(h\supset g \Rightarrow g\in G)}$

3b. Choice (f^{-1} is not empty): $\boxed{\forall f\,\exists\, g\in f^{-1}}$

To Modify ZFC

1. Restrict Replacement to computable R, drop Power Set;
2. add **IP**, $\mathbf{P}\mathcal{X}$, strengthened;
3. extend Foundation to classes of sets (as a family of axioms);
4. some (unclear yet) replacement for Choice.
   (May be dropping it, or adding to the language a postulated (not described) class mapping countable v.Neumann ordinals onto reals, implying continuum hypothesis, too).

Math objects are classes $\{q\colon F_p(q)\}$ of sets q satisfying formulas F with external parameters p. Collections of objects are treated as collections of those parameters, with conditions for Foundation and Extensionality. Quantifiers bind parameters, not properties F.