Set Theory fifty years after Cohen

Patrick Dehornoy

Laboratoire de Mathématiques
Nicolas Oresme, Université de Caen

São Carlos e São Paulo, agosto 2016

Abstract

- Cohen's work is not the end of History.
- Today (much) more is known about (sets and) infinities,
  and there is a reasonable hope that the Continuum Problem will be solved.
- New types of applications of Set Theory appear.

Plan

- I. The Continuum Problem up to Cohen
- II. What does discovering new true axioms mean?
- III. An application of a new type: Laver tables

I. The Continuum Problem up to Cohen

- Theorem (Cantor, 1873): *There exist* *at least two non-equivalent infinities.*

- Theorem (Cantor, 1880's): *There exist* *infinitely many non-equivalent infinities, which organize in a well-ordered sequence*

$$\aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_\omega < \cdots .$$

- Facts. - $\mathrm{card}(\mathbb{N}) = \aleph_0$,
  - $\mathrm{card}(\mathbb{R}) = \mathrm{card}(\mathfrak{P}(\mathbb{N})) = 2^{\aleph_0} > \mathrm{card}(\mathbb{N})$.

- Question (**Continuum Problem**): For which α does $\mathrm{card}(\mathbb{R}) = \aleph_\alpha$ hold?

- Conjecture (**Continuum Hypothesis**, Cantor, 1879): $\mathrm{card}(\mathbb{R}) = \aleph_1$.
  - ▶ Equivalently: every uncountable set of reals has the cardinality of $\mathbb{R}$.

- Theorem (Cantor–Bendixson, 1883): *Closed sets satisfy* CH.

↑
Every closed set of reals either is countable or has the cardinality of $\mathbb{R}$.

- Theorem (Alexandroff, 1916): *Borel sets satisfy* CH.

... and then no progress for 70 years.

- In the meanwhile, formalization of First Order logic (Frege, Russell, ...) and axiomatization of Set Theory (Zermelo, then Fraenkel, ZF):
  - **Consensus**: "*We agree that these properties express our current intuition of sets.*" (*but this may change in the future...*)

- First question: Is CH or ¬CH (negation of CH) provable from ZF?

- <u>Theorem</u> (Gödel, 1938): *Unless* ZF *is contradictory,* $\neg$CH *cannot be proved from* ZF.

  ↑ negation of

- <u>Theorem</u> (Cohen, 1963): *Unless* ZF *is contradictory,* CH *cannot be proved from* ZF.

- Conclusion: ZF is incomplete.
  - Discover further properties of sets, and adopt an **extended list** of axioms!
  - How to recognize that an axiom is true? (What does this mean?)

    Example: CH **may** be taken as an additional axiom, but **not** a good idea...

II. What does discovering new true axioms mean?

- Which new axioms?

- From 1930's, axioms of large cardinal (LC):
  - various solutions to the equation
    $$\frac{\text{super-infinite}}{\text{infinite}} = \frac{\text{infinite}}{\text{finite}}$$
  - **inaccessible** cardinals, **measurable** cardinals, etc.

- Principle: self-similar implies large
  - X **infinite**: $\exists j : X \to X$ (j injective not bijective)
  - X **super**-infinite: $\exists j : X \to X$ (j inject. not biject. preserving all $\in$-definable notions)

    ↑ a **self-embedding** of X
  - Example: No self-embedding of $\mathbb{N}$ may exist, hence $\mathbb{N}$ is not super-infinite.

- Then: LC are natural axioms (iteration of the postulate that infinite sets exist), but no evidence that they are true, or just useful (no connection with ordinary objects).

- Definition: For $A \subseteq \mathbb{R}$, consider the two player $\{0,1\}$-game $\mathbf{G_A}$:

I	a_1		a_3		$\dots$		
II		a_2		a_4		$\dots$	

where I **wins** if the real $[0, a_1 a_2 \dots]_2$ belongs to A.
Then A is called **determined** if one of the players has a winning strategy in G_A.

- An infinitary statement of a special type:

$$\exists a_1 \forall a_2 \exists a_3 \dots ([0, a_1 a_2 \dots]_2 \in A) \textbf{ or } \forall a_1 \exists a_2 \forall a_3 \dots ([0, a_1 a_2 \dots]_2 \notin A),$$

and a model for many properties: there exist codings $\mathbf{C}_{\mathcal{L}}, \mathbf{C}_{\mathcal{B}} : \mathfrak{P}(\mathbb{R}) \to \mathfrak{P}(\mathbb{R})$ s.t.
  A is Lebesgue measurable iff $C_{\mathcal{L}}(A)$ is determined,
  A has the Baire property iff $C_{\mathcal{B}}(A)$ is determined, etc.

- Always true for simple sets and (false) for complicated sets:
  - All closed sets are determined (Gale–Stewart, 1962),
  - All Borel sets are determined (Martin, 1975).
  - "All sets are determined" contradicts AC (Mycielski–Steinhaus, 1962),
  - "All **projective** sets are determined" unprovable from ZF ($\approx$ Gödel, 1938).

  $\uparrow$ closure of Borel sets under continuous image and complement

- Definition: Axiom of **Projective Determinacy** (PD):
  "Every projective set of reals is determined".

- Propositions (Moschovakis, Kechris, ..., 1970s): *When added to* ZF,
  PD *provides a complete and satisfactory description of projective sets of reals.*

  ↑ heuristically complete ↑ no pathologies: Lebesgue measurable, etc.

  - Example: Under ZF + PD, projective sets satisfy CH.

- So: PD is useful (gives a better description of usual sets),
  but not natural (why consider it?),
  contrary to large cardinal axioms, which are natural but (a priori) not useful.

- Theorem (Martin–Steel 1985, Woodin, 1987): PD *is a large cardinal axiom.*

  ↑ infinitely many Woodin cardinals imply PD

  ↑ PD (implies) infinitely many Woodin cardinals

- Corollary (Woodin): PD *is true.*

  "Proof": PD is both natural (as a large cardinal axiom), and useful (as a determinacy property). □

- Why "**true**"?
  - ▶ Compare with the axiom of infinity:
    Evidence = (?) interiorization of a long familiarity and of practical efficiency.
  - ▶ (Woodin) *"The statement that* PD *is consistent is a new mathematical truth. It predicts facts about our world, for instance that in the next 1000 years there will be no contradiction discovered from PD by any means."*
  - ▶ New consensus: The base system for 21th century Set Theory is no longer ZF, but ZF + PD.

- Fact: CH and ¬CH not provable from ZF + PD: description not yet complete...
  - with ZF: (heuristically) complete description of finite sets;
  - with ZF+PD: (heuristically) complete description of finite and countable sets;
  - with ZF+PD+??: (heuristically) complete description of sets up to cardinal $\aleph_1$:

    ... which will necessarily entail a solution to CH.

- Currently most promising approach: identify one canonical reference universe.

  (think of $\mathbb{C}$ in the world of number fields of characteristic 0)
  - a typical candidate: Gödel's universe L of constructible sets (1938).

    ↑ the minimal universe: only definable sets (think of the prime field $\mathbb{Q}$)
  - fully understood ("**fine structure theory**", Jensen and Silver, 1970s), but cannot be the reference universe because
    - incompatible with large cardinals: contradicts PD,
    - implies pathologies: existence of a non-measurable projective subset of $\mathbb{R}$...

- Question: Can one find an L-like universe compatible with large cardinals?

- The inner model program (in the world of fields: constructing algebraic closure...)
  - ▶ universe $L[U]$ (Kunen, 1971): compatible with one measurable cardinal;
  - ▶ universe $L[E]$ (Mitchell–Steel, 1980-90s): compatible with PD;
  - ▶ but: how could this be completed with an endless hierarchy of large cardinals?

- Theorem (Woodin, 2006): *There exists an explicit level (one* **supercompact** *cardinal) such that, if an L-like universe is compatible with large cardinals up to that level, it is automatically compatible with all large cardinals.*

- Conjecture (Woodin, 2010): ZF + PD+V=**ultimate-L** *is true.*

↑ the L-like universe for one supercompact

▶ means proving that V=ultimate-L is both natural (an aesthetic judgment based on cumulated experience...) and useful (= provides a description with no pathologies)

- Proposition: ZF + PD+V=ultimate-L *implies* GCH.

▶ If ZF + PD+V=ultimate-L becomes accepted as the base of Set Theory, then the Continuum Problem will have been solved.

III. An application of a new type: Laver tables

- The (left) selfdistributivity law:

$$x * (y * z) = (x * y) * (x * z). \qquad \text{(LD)}$$

  - Classical example 1: E module and $x * y := (1-\lambda)x + \lambda y$;
  - Classical example 2: G group and $x * y := xyx^{-1}$.
    NB: all idempotent ($x * x = x$), hence no nontrivial monogenerated structure
  - (Brieskorn,...) Algebraic counterpart of Reidemeister move III...

- A binary operation on $\{1, 2, 3, 4\}$: the four element **Laver table**

$*$	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

- Start with $+1 \bmod 4$ in the first column,
  and complete so as to obey the rule $x * (y * 1) = (x * y) * (x * 1)$:

$$4 * 2 = 4 * (1 * 1) = (4 * 1) * (4 * 1) = 1 * 1 = 2,$$
$$4 * 3 = 4 * (2 * 1) = (4 * 2) * (4 * 1) = 2 * 1 = 3,$$
$$4 * 4 = 4 * (3 * 1) = (4 * 3) * (4 * 1) = 3 * 1 = 4,$$
$$3 * 2 = 3 * (1 * 1) = (3 * 1) * (3 * 1) = 4 * 4 = 4, \ldots$$

- The same construction works for every size:

- Proposition (Laver): (i) *For every* N, *there exists a unique binary operation* $*$ *on* $\{1, ..., N\}$ *satisfying*

$$x * 1 = x + 1 \bmod N \quad \text{and}$$
$$x * (y * 1) = (x * y) * (x * 1).$$

(ii) *The operation thus obtained obeys the LD-law if and only if* N *is a power of* 2.

  - A_n := the **Laver table** with 2^n elements.

- For $n \geqslant 1$, one has $1 * 1 = 2 \neq 1$ in A_n: not idempotent.
  - quite different from group conjugacy and other classical LD-structures
  - a counterpart of cyclic groups $\mathbb{Z}/n\mathbb{Z}$ in the selfdistributive world:
    A_n presented by $\langle 1 \mid 1_{[2^n]} = 1 \rangle_{LD}$, with $x_{[p]} = (...((x * x) * x)...) * x$, p terms.

A_0	1
1	1

A_1	1	2
1	2	2
2	1	2

A_2	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

A_4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	12	14	16	2	12	14	16	2	12	14	16	2	12	14	16
2	3	12	15	16	3	12	15	16	3	12	15	16	3	12	15	16
3	4	8	12	16	4	8	12	16	4	8	12	16	4	8	12	16
4	5	6	7	8	13	14	15	16	5	6	7	8	13	14	15	16
5	6	8	14	16	6	8	14	16	6	8	14	16	6	8	14	16
6	7	8	15	16	7	8	15	16	7	8	15	16	7	8	15	16
7	8	16	8	16	8	16	8	16	8	16	8	16	8	16	8	16
8	9	10	11	12	13	14	15	16	9	10	11	12	13	14	15	16
9	10	12	14	16	10	12	14	16	10	12	14	16	10	12	14	16
10	11	12	15	16	11	12	15	16	11	12	15	16	11	12	15	16
11	12	16	12	16	12	16	12	16	12	16	12	16	12	16	12	16
12	13	14	15	16	13	14	15	16	13	14	15	16	13	14	15	16
13	14	16	14	16	14	16	14	16	14	16	14	16	14	16	14	16
14	15	16	15	16	15	16	15	16	15	16	15	16	15	16	15	16
15	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

• Proposition (Laver): *For every $p \leqslant 2^n$, there exists a number $\pi_n(p)$, a power of 2, such that the pth row of A_n is the periodic repetition of $\pi_n(p)$ values increasing from $p{+}1 \bmod 2^n$ to 2^n.*

• Example:

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

- $\pi_3(1) = 4$
- $\pi_3(2) = 4$
- $\pi_3(3) = 2$
- $\pi_3(4) = 4$
- $\pi_3(5) = 2$
- $\pi_3(6) = 2$
- $\pi_3(7) = 1$
- $\pi_3(\mathbf{8}) = 8$

• A few values of the periods of 1 and 2:

n	0	1	2	3	4	5	6	7	8	9	10	11	⋯
$\pi_n(1)$	1	1	2	4	4	8	8	8	8	16	16	16	⋯
$\pi_n(2)$	–	2	2	4	4	8	8	16	16	16	16	16	⋯

- Question 1: Does $\pi_n(2) \geqslant \pi_n(1)$ always hold?
- Question 2: Does $\pi_n(1)$ tend to ∞ with n? Does it reach 32?

- Theorem (Laver, 1995): *If there exists a selfsimilar set, then the answer to the above questions is positive.*

- Definition: A **rank** is a set R such that $f : R \to R$ implies $f \in R$. (this exists...)

- Assume that X is selfsimilar (i.e., ∃ self-embedding of X):
  - then there exists a selfsimilar rank, say R;
  - if i, j are self-embeddings of R, then $i : R \to R$ and $j \in R$, hence we can **apply** i to j;
  - "being a self-embedding" is definable from $\in$, hence $i(j)$ is a self-embedding;
  - "being the image of" is definable from $\in$,
    hence $\ell = j(k)$ implies $i(\ell) = i(j)(i(k))$, i.e., $i(j(k)) = i(j)(i(k))$: LD-law.

- Proposition (Laver): *Assume j is a self-embedding of a rank R.*
  (i) The set Iter(j) *of* **iterates** *of j (i.e., j, $j(j)$, $j(j)(j)$...) obeys the LD-law.*
  (ii) For every n, there exists a compatible equivalence relation on Iter(j) *with 2^n classes and the first column of its table is a cycle, hence the quotient is A_n.*
  (iii) For $m \leqslant n$ and $p \leqslant 2^n$, the period of p jumps from 2^m to 2^{m+1} between A_n and A_{n+1} iff $j_{[p]}$ maps crit$(j_{[2^m]})$ *to* crit$(\mathrm{j}_{[2^n]})$.

↑
the first ordinal moved by...

- Lemma: *If j is a self-embedding, then $j(j)(\alpha) \leqslant j(\alpha)$ holds for every ordinal α.*

  - Proof: There exists β satisfying $j(\beta) > \alpha$, hence there is a smallest such β, which therefore satisfies $j(\beta) > \alpha$ and
  $$\forall \gamma < \beta \; (j(\gamma) \leqslant \alpha). \qquad (*)$$
  Applying j to $(*)$ gives
  $$\forall \gamma < j(\beta) \; (j(j)(\gamma) \leqslant j(\alpha)). \qquad (**)$$
  Taking $\gamma = \alpha$ in $(**)$ yields $j(j)(\alpha) \leqslant j(\alpha)$. □

- Proposition (Laver): *If there exists a selfsimilar set, $\pi_n(2) \geqslant \pi_n(1)$ holds for every n.*

- Similar (more difficult) proof for Question 1 (period of 1 in A_n tends to ∞).

- Alternative proofs without the large cardinal assumption? Not yet...
  - partial results by Drápal... but no complete proof so far:
  - a strange situation: why a connection between finite tables and large cardinals?

- Set Theory is a theory of infinity: its aim is to explore the various possible infinities.
  (nothing less, nothing more: "New Math" was a misunderstanding...)

- History continues:
  - A coherent theory beyond ZF is possible;
  - There is a consensus about enriching ZF into ZF+PD;
  - The next step should include a solution of the Continuum Problem.

- A last question: Are the properties of Laver tables an application of Set Theory?
  - **So far**, yes; **later**, formally no if one finds alternative proofs without Set Theory.
  - But, **in any case**, it is Set Theory that made the properties first accessible...
  - An analogy: In physics: using a physical intuition, guess statements, then pass them to the mathematician for a formal proof; Here: using a logical intuition (existence of a selfsimiliar set), guess statements (periods in Laver tables tend to ∞), then pass them to the mathematician for a formal proof.
  - No need to believe in the existence of large cardinals to use them...

- W. Hugh Woodin, *Strong axioms of infinity and the search for V*,
  Proceedings ICM Hyderabad 2010, pp. 504–528

- R. Laver, *On the algebra of elementary embeddings of a rank into itself*,
  Adv. in Math. 110 (1995) 334–346

- P. Dehornoy, *Laver's results and low-dimensional topology*,
  Arch. Math. Logic, 55 (2016) 49–83.

- P. Dehornoy & V. Lebed, *Two- and three-cocycles for Laver tables*,
  J. Knot Theory and Ramifications, 23-4 (2014) 1450017

www.math.unicaen.fr/∼dehornoy

... Muito obrigado e da próxima vez !