Wetzel: Formalisation of an Undecidable Problem Linked to the Continuum Hypothesis

Lawrence C Paulson FRS

CICM 2022, Tbilisi

Supported by the ERC Advanced Grant ALEXANDRIA (Project GA 742178).

Background

Suppose that F is a family of analytic functions on $\mathbb{C}$ such that for each z the set $\{f(z) : f \in F\}$ is countable. (Call this property P_0.) Then is the family F itself countable?

Posed by John E Wetzel; settled by Paul Erdős, who discovered it in a problem book at Ann Arbor University.

*The answer is **yes** iff the Continuum Hypothesis is **false**.*

Can we formalise something that requires both complex analysis and transfinite constructions?

The Continuum Hypothesis (CH)

- Asserts that there is no cardinal between $\aleph_0$ and $2^{\aleph_0}$ (between the cardinalities of the *integers* and the *reals*)
- *Or*: every subset of $S \subseteq \mathbb{R}$ can be embedded into $\mathbb{N}$, or else $\mathbb{R}$ can be embedded into S
- One of the most celebrated questions in mathematics, it's *independent* of the axioms of set theory.

Isabelle and Set Theory

- **Isabelle/ZF** is a possible basis for ambitious set theory developments, but lacks vital automation and libraries
- **Isabelle/HOL** has those, but higher-order logic (HOL) is *much* weaker than Zermelo-Fraenkel set theory
- Fortunately, it's easy to **add** set theory to HOL, thanks to prior work by Gordon and Obua
- HOL+ZF is stronger than ZF; weaker than ZF+Con(ZF)

The ZFC-in-HOL Library

- The usual ZF axioms, with `V` as the type of all sets
- Integration with Isabelle/HOL:
  - *overloading* the lattice symbols ⊓, ⊔, ≤, etc.
  - type `V set` as the type of ZF classes
  - identifying "small" sets and types
  - defining cardinality, etc., for *all* small sets
  - associating ZF sets with small types, e.g. `complex`

Formalisation

Wetzel: The ¬CH Case

Defining Wetzel's property P_0

```
definition Wetzel :: "(complex ⇒ complex) set ⇒ bool"
  where "Wetzel ≡ λF. (∀f∈F. f analytic_on UNIV) ∧ (∀z. countable((λf. f z) ` F))"
```

The theorem statement, assuming ¬CH

```
proposition Erdos_Wetzel_nonCH:
  assumes W: "Wetzel F" and NCH: "C_continuum > ℵ1"
  shows "countable F"
```

It's enough to show the contrapositive:

```
have "∃z0. gcard ((λf. f z0) ` F) ≥ ℵ1" if "uncountable F"
```

The ¬CH Case (Continued)

F is uncountable, so obtain a subset F' of cardinality $\aleph_1$
and an enumeration $\phi : \omega_1 \to F'$

```
have "gcard F ≥ ℵ1"
  using that uncountable_gcard_ge by force
then obtain F' where "F' ⊆ F" and F': "gcard F' = ℵ1"
  by (meson Card_Aleph subset_smaller_gcard)
then obtain φ where φ: "bij_betw φ (elts ω1) F'"
  by (metis TC_small eqpoll_def gcard_eqpoll)
```

We define $S(\alpha, \beta)$, the set of points where ϕ_α and ϕ_β agree,
and show it's countable for ordinals $\alpha < \beta < \omega_1$

```
define S where "S ≡ λα β. {z. φ α z = φ β z}"
have "gcard (S α β) ≤ ℵ0" if "α ∈ elts β" "β ∈ elts ω1" for α β
```

(Holomorphic functions that agree on an uncountable set are equal)

The ¬CH Case (Finish)

Now define the **union** of all $S(\alpha, \beta)$ for $\alpha < \beta < \omega_1$. Clearly $SS \subseteq \mathbb{C}$

```
define SS where "SS ≡⨆β ∈ elts ω1. ⨆α ∈ elts β. S α β"
```

We can show $|SS| \leq \aleph_1$. Since ¬CH there exists some $z_0 \notin SS$.

```
finally have "gcard SS ≤ ℵ1" .
with NCH obtain z0 where "z0 ∉ SS"
  by (metis Complex_gcard UNIV_eq_I less_le_not_le)
```

∴ the uncountably many functions in F' return distinct values for z_0

And that's basically it! The whole proof is 50 lines.

The Case Where CH Holds

Since $|\mathbb{C}| = \aleph_1$, write $\mathbb{C} = \{\zeta_\alpha : \alpha < \omega_1\}$, *indexing* the complex numbers

Consider the *rational* complex numbers $D = \{p + iq : p, q \in \mathbb{Q}\}$.

Construct *distinct* functions $\{f_\beta : \beta < \omega_1\}$ such that $f_\beta(\zeta_\alpha) \in D$ if $\alpha < \beta$

Any such uncountable family contradicts P_0

We construct each f_γ from its predecessors by *transfinite induction,*
assuming that distinct functions $\{f_\beta : \beta < \gamma\}$ already exist

The Key Construction

The ordinal γ is countable, so we can enumerate

$\{f_\beta : \beta < \gamma\}$ as $\{g_0, g_1, \ldots\}$ and $\{\zeta_\alpha : \alpha < \gamma\}$ as $\{w_0, w_1, \ldots\}$.

Then define

$$f_\gamma(z) := \epsilon_0 + \epsilon_1(z - w_0) + \epsilon_2(z - w_0)(z - w_1) + \cdots$$

for suitable ϵ_0, ϵ_1, ϵ_2, … chosen *sequentially*.

In the easy case, γ is finite and f_γ is just a polynomial. Otherwise, care is needed to make it converge—to suitable values!

Formalising the CH Case

```
proposition Erdos_Wetzel_CH:
  assumes CH: "C_continuum = ℵ1"
  obtains F where "Wetzel F" and "uncountable F"
```

We define D, which is countable, infinite and dense in $\mathbb{C}$

```
define D where "D ≡ {z. Re z ∈ ℚ ∧ Im z ∈ ℚ}"
have Deq: "D = (⋃x∈ℚ. ⋃y∈ℚ. {Complex x y})"
  using complex.collapse by (force simp: D_def)
with countable_rat have "countable D"
  by blast
```

```
then have cloD: "closure D = UNIV"
  by (auto simp: D_def closure_approachable dist_complex_def)
```

Here we index the complex numbers as $\{\zeta_\alpha : \alpha < \omega_1\}$

```
obtain ζ where ζ: "bij_betw ζ (elts ω1) (UNIV::complex set)"
  by (metis Complex_gcard TC_small assms eqpoll_def gcard_eqpoll)
```

The transfinite construction

We are given $\{f_\beta : \beta < \gamma\}$, a family of *distinct* analytic functions

```
have f: "∀β ∈ elts γ. f β analytic_on UNIV ∧ inD β (f β)"
  using that by (auto simp: Φ_def)
have inj: "inj_on f (elts γ)"
  using that by (simp add: Φ_def inj_on_def) (meson Ord_ω1 Ord_in_Ord Ord_linear)
```

In the finite case, γ is some natural number n. The construction of f_γ (called here h) involves a **nested** induction on n. It almost fits on a slide!

```
have **: "∃h. h analytic_on UNIV ∧ (∀i<n. h (w i) ∈ D ∧ h (w i) ≠ g i (w i))"
  if "n ≤ card (elts γ)" for n
  using that
proof (induction n)
  case 0
  then show ?case
    using analytic_on_const by blast
next
  case (Suc n)
  then obtain h where "h analytic_on UNIV" and hg: "∀i<n. h(w i) ∈ D ∧ h(w i) ≠ g i (w i)"
    using Suc_leD by blast
  define p where "p ≡ λz. ∏i<n. z - w i"
  have p0: "p z = 0 ⟷ (∃i<n. z = w i)" for z
    unfolding p_def by force
  obtain d where d: "d ∈ D - {g n (w n)}"
    using ‹infinite D› by (metis ex_in_conv finite.emptyI infinite_remove)
  define h' where "h' ≡ λz. h z + p z * (d - h (w n)) / p (w n)"
  have h'_eq: "h' (w i) = h (w i)" if "i<n" for i
    using that by (force simp: h'_def p0)
  show ?case
  proof (intro exI strip conjI)
    have nless: "n < card (elts γ)"
      using Suc.prems Suc_le_eq by blast
    with η have "η n ≠ η i" if "i<n" for i
      using that unfolding bij_betw_iff_bijections
      by (metis lessThan_iff less_not_refl order_less_trans)
    with ζ η γ have pwn_nonzero: "p (w n) ≠ 0"
      apply (clarsimp simp: p0 w_def bij_betw_iff_bijections)
      by (metis Ord_ω1 Ord_trans nless lessThan_iff order_less_trans)
    then show "h' analytic_on UNIV"
      unfolding h'_def p_def by (intro analytic_intros ‹h analytic_on UNIV›)
    fix i
    assume "i < Suc n"
    then have §: "i < n ∨ i = n"
      by linarith
    then show "h' (w i) ∈ D"
      using h'_eq hg d h'_def pwn_nonzero by force
    show "h' (w i) ≠ g i (w i)"
      using § h'_eq hg h'_def d pwn_nonzero by fastforce
  qed
qed
```

old h by induction hyp

new $d \in D$ for w_n, diagonalising

new h' agrees with h on w_i, $i < n$

$h'(w_i)$ is correct for $i < n + 1$

If $\gamma \geq \omega$, define an infinite sum

The ordinals below γ indexed as $\eta_0, \eta_1, \eta_2, \ldots$

```
case False
then obtain η where η: "bij_betw η (UNIV::nat set) (elts γ)"
  by (meson γ countable_infiniteE' less_ω1_imp_countable)
```

The f and ζ sequences similarly indexed by natural numbers

```
define g where "g ≡ f o η"
define w where "w ≡ ζ o η"
```

From those, we start setting up a summable series:

```
define p where "p ≡ λn z. ∏i<n. z - w i"
define q where "q ≡ λn. ∏i<n. 1 + norm (w i)"
define h where "h ≡ λn ε z. ∑i<n. ε i * p i z"
define BALL where "BALL ≡ λn ε. ball (h n ε (w n)) (norm (p n (w n)) / (fact n * q n))"
```

We ensure membership in D; freshness will be by diagonalisation

```
define DD where "DD ≡ λn ε. D ∩ BALL n ε - {g n (w n)}"
define dd where "dd ≡ λn ε. SOME x. x ∈ DD n ε"
```

Recursive defn of $\epsilon_0, \epsilon_1, \epsilon_2, \ldots,$

Well-founded recursion, where ε will be replaced by `coeff`

```
define coeff where "coeff ≡ wfrec less_than (λε n. (dd n ε - h n ε (w n)) / p n (w n))"
```

Recursive unfolding allows `dd` and `h` to refer to earlier coefficients

```
have coeff_eq: "coeff n = (dd n coeff - h n coeff (w n)) / p n (w n)" for n
  by (simp add: def_wfrec [OF coeff_def])
```

We need to show that the ϵ_i decrease rapidly

```
have norm_coeff: "norm (coeff n) < 1 / (fact n * q n)" for n
```

Finally: the "next" function

hh denotes $f_\gamma(z)$ which is $\epsilon_0 + \epsilon_1(z - w_0) + \epsilon_2(z - w_0)(z - w_1) + \cdots$, and it's holomorphic because it's the uniform limit of polynomials

```
define hh where "hh ≡ λz. suminf (λi. coeff i * p i z)"
have "hh holomorphic_on UNIV"
```

This claim is the required $f_\gamma(\zeta_\alpha) \in D$ if $\alpha < \gamma$

```
then have "hh (w n) ∈ D" for n
  using DD_def dd_in_DD by fastforce
```

This claim is that f_γ is fresh, so that the family will be large enough

```
then show "∀β∈elts γ. hh ≠ f β"
  by (metis η bij_betw_imp_surj_on imageE)
```

That completes the transfinite construction. We need another 50 lines of boilerplate and routine checks to wind up the proof.

The formalisation has a **de Bruijn factor** < 3

Discussion

Machine proofs: a timeline

2003: relative consistency of AC

2005: four-colour theorem

2012: odd-order theorem

2013: incompleteness theorems

2014: Kepler conjecture

2014: central limit theorem

2019: perfectoid spaces

2021: schemes (in Lean and Isabelle/HOL)

2022: Liquid Tensor Experiment

A shift from long proofs about simple objects to **attempting to work** *with sophisticated objects*

So what do we get from Wetzel?

- 360 lines: a short proof and no “sophisticated objects”
- but a nontrivial interplay between
  - *set theory*: cardinal numbers, transfinite recursion
  - *analysis*: holomorphic functions, Weierstrass *M*-test
- no difficulty combining the two vernaculars

The future

- How about some harder problems combining these two domains?
- And did this exercise decrease my Erdős number?