Wetzel:
Formalisation of an Undecidable Problem Linked to the Continuum Hypothesis
Lawrence C Paulson FRS

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 \( \mathcal{V} \) as the type of all sets

Integration with Isabelle/HOL:
- *overloading* the lattice symbols \( \sqcap, \sqcup, \leq, \) etc.
- type \( \mathcal{V} \text{ set} \) 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 \(\neg CH\) Case

Defining Wetzel's property \(P_0\)

**definition** Wetzel :: "(complex \(\Rightarrow\) complex) set \(\Rightarrow\) bool"

**where** "Wetzel \(\equiv\) \(\lambda\) F. (\(\forall\) f \(\in\) F. f analytic_on UNIV) \& (\(\forall\) z. countable((\(\lambda\) f. f z) \` F))"

The theorem statement, assuming \(\neg CH\)

**proposition** Erdos_Wetzel_nonCH:

**assumes** W: "Wetzel F" and NCH: "C_continuum > \(\aleph_1\)"

**shows** "countable F"

It's enough to show the contrapositive:

**have** "\(\exists\) z \(\theta\). gcard ((\(\lambda\) f. f z\(\theta\)) \` F) \(\ge\) \(\aleph_1\)" if "uncountable F"
The $\neg$CH Case (Continued)

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

```plaintext
have "gcard F ≥ \aleph_1"
  using that uncountable_gcard_ge by force
then obtain F' where "F' ⊆ F" and F': "gcard F' = \aleph_1"
  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 $\phi_\alpha$ and $\phi_\beta$ agree, and show it’s countable for ordinals $\alpha < \beta < \omega_1$

```plaintext
define S where "S ≡ ∀α, β. {z. ϕ α z = ϕ β z}"
have "gcard (S α β) ≤ \aleph_0" if "α ∈ elts β" "β ∈ elts ω1" for α β
```

(Holomorphic functions that agree on an uncountable set are equal)
The $\neg$CH Case (Finish)

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

```plaintext
define SS where "SS = \bigsqcup \beta \in \text{elts } \omega_1. \bigsqcup \alpha \in \text{elts } \beta. S(\alpha, \beta)"
```

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

```plaintext
finally have "gcard SS \leq \aleph_1" .
with NCH obtain z0 where "z0 \notin 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 $f_\gamma$ from its predecessors by transfinite induction, assuming that distinct functions $\{f_\beta : \beta < \gamma\}$ already exist
The Key Construction

The ordinal $\gamma$ 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 $\epsilon_0, \epsilon_1, \epsilon_2, \ldots$ chosen sequentially.

In the easy case, $\gamma$ is finite and $f_\gamma$ is just a polynomial. Otherwise, care is needed to make it converge—to suitable values!
Formalising the CH Case

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

```
proposition Erdos_Wetzel_CH: 
  assumes CH: "C_continuum = \aleph_1"
  obtains F where "Wetzel F" and "uncountable F"
```

define $D$ where "$D \equiv \{z. \text{Re } z \in \mathbb{Q} \land \text{Im } z \in \mathbb{Q}\}"
have Deq: "D = (\bigcup x \in \mathbb{Q}. \bigcup y \in \mathbb{Q}. \{\text{Complex } x \times y\})"
  using complex.collapse by (force simp: D_def)
with countable_rat have "countable $D"
  by blast
then have cloD: "closure $D = \text{UNIV}"
  by (auto simp: D_def closure_approachable dist_complex_def)

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

```
obtain \zeta where \zeta: "bij_betw \zeta (elts \omega_1) (UNIV::\text{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

```plaintext
have f: "\( \forall \beta \in \text{elts } \gamma. \ f \beta \text{ analytic on UNIV } \land \text{inD } \beta (f \beta)\)"
  using that by (auto simp: \( \Phi \)_def)
have inj: "\(\text{inj on f (elts } \gamma)\)"
  using that by (simp add: \( \Phi \)_def inj_on_def) (meson Ord_\( \omega 1 \) Ord_in Ord Ord_linear)
```

In the finite case, \( \gamma \) is some natural number \( n \). The construction of \( f_\gamma \) (called here \( h \)) involves a nested induction on \( n \). It almost fits on a slide!
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 $\gamma$ indexed as $\eta_0, \eta_1, \eta_2, \ldots$

```plaintext
case False
then obtain \( \eta \) where \( \eta: \text{bij_betw} \ \eta \ \text{(UNIV::nat set)} \ \text{(elts } \gamma) \)
by (meson \( \gamma \ \text{countable_infiniteE} \ \text{less_}\omega1\_imp\_countable)"
```

The $f$ and $\zeta$ sequences similarly indexed by natural numbers

```plaintext
define g where "g \equiv f \circ \eta"
define w where "w \equiv \zeta \circ \eta"
```

From those, we start setting up a summable series:

```plaintext
define p where "p \equiv \lambda n\ z. \ \Pi_{i<n}.\ z - w\ i"
define q where "q \equiv \lambda n. \ \Pi_{i<n}.\ 1 + \text{norm} \ (w\ i)"
define h where "h \equiv \lambda n \ \epsilon\ z. \ \Sigma_{i<n}.\ \epsilon\ i \ast p\ i\ z"
define BALL where "BALL \equiv \lambda n \ \epsilon. \ \text{ball} \ (h\ n\ \epsilon\ (w\ n))\ (\text{norm} \ (p\ n\ (w\ n)) \ / \ (\text{fact} \ n \ * \ q\ n))"
```

We ensure membership in $D$; freshness will be by diagonalisation

```plaintext
define DD where "DD \equiv \lambda n \ \epsilon. \ D \cap \text{BALL} \ n\ \epsilon\ - \ \{g\ n\ (w\ n)\}"
define dd where "dd \equiv \lambda n \ \epsilon. \ \text{SOME} \ x. \ x \in DD \ n\ \epsilon"
```
Recursive defn of $\epsilon_0$, $\epsilon_1$, $\epsilon_2$, ..., 

Well-founded recursion, where $\epsilon$ will be replaced by `coeff`

```lean
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

```lean
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 $\epsilon_i$ decrease rapidly

```lean
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 $f_{\gamma}$ 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?