数理解析研究所講究録
第 1790 巻 2012 年 10-15

Notes on an old theorem of Erdős concerning CH

Hiroshi Fujita (藤田 博司)
Ehime University

February 2012

Introduction

Let us discuss, in this article, some observations about one very old theorem due to Paul Erdős.

Let $\mathcal{H}$ be the set of all entire functions, that is to say, complex-valued functions which are defined on the whole complex plane $\mathbb{C}$ and are holomorphic everywhere. Given $\mathcal{A} \subset \mathcal{H}$ and $z \in \mathbb{C}$, we put $\mathcal{A}(z) = \{ f(z) : f \in \mathcal{A} \}$.

Let us say $\mathcal{A} \subset \mathcal{H}$ has the *property* P_0 if and only if $\mathcal{A}(z)$ is countable for every $z \in \mathbb{C}$. Clearly every countable subset of $\mathcal{H}$ has property P_0. Whether there is an uncountable set which possesses property P_0 is independent of conventional axioms of set theory. In fact, Erdős have shown

THEOREM 0. (Erdős, see [1]) *There is an uncountable subset of* $\mathcal{H}$ *having the property* P_0 *if and only if CH (the Continuum Hypothesis) holds.*

We review Erdős' argument and give the following

THEOREM 1. *There is no uncountable* $\mathbf{\Sigma}^1_1$ *set with property* P_0.

THEOREM 2. *If there is an uncountable* $\mathbf{\Sigma}^1_2$ *set with property* P_0*, then there is a real* $r \subset \omega$ *from which every real is constructible:* $\mathbb{R} \subset L[r]$.

THEOREM 3. *If there is a real* $r \subset \omega$ *such that* $\mathbb{R} \subset L[r]$*, then there is an uncountable* $\mathbf{\Pi}^1_1$ *set with property* P_0.

But before proving any of these, we should explain how to equip $\mathcal{H}$ as a Polish space. We do this in the next section. Then in section 2 we give proof of our Theorems 1 and 2. In section 3 we give a detailed review of "if" part of Erdős' argument and show how to apply Arnie Miller's trick to derive Theorem 3.

This article is based on a seminar talk I gave at Kobe Univeristy in a meeting held on February 21–23. I would like to thank all the participants.

1 Polish topology on the entire functions

For each non-negative integer n put

$$d_n(f,g) = \sup\{ |f(z) - g(z)| : z \in \mathbb{C},\ |z| \leq n \} \qquad (f, g \in \mathcal{H}).$$

By virtue of the uniqueness theorem of holomorphic functions ([4, Theorem 10.18]), d_n is a metric on $\mathcal{H}$ for each $n \geq 1$. But none of these metrics is complete. Every d_n-Cauchy sequence of members in $\mathcal{H}$ converges to a function which is continuous on the closed disk $\overline{D}(0;n) = \{ z \in \mathbb{C} : |z| \leq n \}$ and is holomorphic inside that disk. But the limit function may fail to inherit the possibility of analytic continuation to the whole plane. In order to make sure that the limit function is holomorphic everywhere, we need to require sequence to be convergent in all d_n's.

Now let us put

$$d(f,g) = \sum_{n=0}^{\infty} \frac{d_n(f,g)}{2^{n+1}(1+d_n(f,g))} \qquad (f,g \in \mathcal{H}).$$

Then d is a complete metric which gives $\mathcal{H}$ the topology of uniform convergence on compact sets. See [4, Theorem 10.28]. On the other hand, $\mathcal{H}$ is separable under this topology since polynomials with rational coefficients form a countable dense set.

To summarize: $\mathcal{H}$ is a Polish space under the topology of uniform convergence on compact sets.

In our proof of Theorem 2, we need to think each entire function as a *real*. If you take (as every textbook of set theory does) functions as sets of ordered pairs, the assertion *"f is constructible"* doesn't make sense unless the whole domain is constructible. But when we say a holomorphic function f to be constructible, we would like to mean it is defined using a constructible set of informations, without implying that the whole $\mathbb{C}$ is contained in L. So we identify each function $f \in \mathcal{H}$ with its power-series expansion at the origin:

$$f(z) = c_0 + c_1 z + c_2 z^2 + \cdots + c_k z^k + \cdots .$$

We say f to be constructible when the sequence $\langle c_k : k \in \omega \rangle$ is constructible in the usual sense. Thus we identify f with a sequence of complex numbers when we talk about definability aspect of numbers and functions.

2 Proof of Theorems 1 and 2

Our proof of Theorem 1 is just a straightforward absoluteness argument.

Suppose we are given a Σ^1_1 formula $\varphi(x)$ (possibly containing some reals as parameters) which talks about an element x of a fixed Polish space X. We can form an assertion

Φ: "The set $\{ x \in X : \varphi(x) \}$ is uncountable."

Let us see that Φ is a Σ^1_2 sentence with the same parameters as $\phi(x)$.

We can extract from φ the definition of a continuous function F of ${}^\omega\omega$ onto $\{ x \in X : \varphi(x) \}$. By tracing a proof of Suslin's perfect set theorem, we know Φ holds if and only if there exists a system $\{ N_s : s \in {}^{<\omega}2 \}$ of basic neighbourhoods in ${}^\omega\omega \times X$ such that

(1) $\overline{N_{s^\frown(i)}} \subset N_s$ for $s \in {}^{<\omega}2$ and $i \in \{0,1\}$,
(2) the diameter of N_s is less than or equal to $2^{-\text{length}(s)}$,
(3) the projections onto X of $N_{s^\frown(0)}$ and $N_{s^\frown(1)}$ are disjoint, and
(4) the closed set determined by $\{ N_s : s \in {}^{<\omega}2 \}$:

$$C = \bigcup_{\sigma \in {}^\omega 2} \bigcap_{n \in \omega} \overline{N_{\sigma|n}}$$

is contained in the graph of the continuous function F.

The assertion of existence of such system $\{ N_s : s \in {}^{<\omega}2 \}$ of neighbourhoods is easily seen to be Σ^1_2 uniformly in the formula $\varphi(x)$.[*1]

Now suppose we are given a $\mathbf{\Sigma}^1_1$ set $\mathcal{A} \subset \mathcal{H}$. Then two assertions,

$$\Phi_1\text{: “}\mathcal{A}\text{ is uncountable”}$$

and

$$\Phi_2\text{: “there is } z \in \mathbb{C} \text{ at which the section } \mathcal{A}(z) \text{ is uncountable”}$$

are both $\mathbf{\Sigma}^1_2$.

By Erdős' theorem we know

$$\neg\mathrm{CH} \rightarrow (\Phi_1 \rightarrow \Phi_2).$$

The statement $\Phi_1 \rightarrow \Phi_2$ is absolute for every generic extension since it is a Boolean combination of $\mathbf{\Sigma}^1_2$ sentences (by the Shoenfield Absoluteness Theorem.) We also know that $\neg$CH is forceable by the poset of finite partial functions from (a subset of) ω_2 into ω. From this it follows that $\Phi_1 \rightarrow \Phi_2$ holds in the universe V. Therefore, each time we are given a $\mathbf{\Sigma}^1_1$ subset $\mathcal{A} \subset \mathcal{H}$, we have either that $\mathcal{A}$ is countable or else that $\mathcal{A}$ lacks the property P_0. This completes our proof of Theorem 1.

Let us note, as a corollary of Theorem 1, that a subset $\mathcal{H}$ with property P_0 can never has a perfect subset.

Now, in order to prove Theorem 2, suppose we are given an uncountable $\mathbf{\Sigma}^1_2$ set $\mathcal{A} \subset \mathcal{H}$ which has property P_0. Suppose $\mathcal{A}$ is Σ^1_2 definable using, say, a parameter $r \subset \omega$. Then we show that every complex number $z \in \mathbb{C}$ is in $L[r]$. We do this by recalling “only if” part of Erdős' argument.

For $f, g \in \mathcal{H}$ let $S(f,g) = \{ z \in \mathbb{C} : f(z) = g(z) \}$. If $f \neq g$ then by virtue of the uniqueness theorem of holomorphic functions $S(f,g)$ does not have an accumlating point anywhere on $\mathbb{C}$. It follows that $S(f,g)$ is countable if $f \neq g$.

If $\mathcal{A} \subset \mathcal{H}$ is uncountable and has property P_0, then the mapping

$$f \mapsto f(z)$$

can never be one-to-one on $\mathcal{A}$ for any fixed $z \in \mathbb{C}$. So for every $z \in \mathbb{C}$ there are $f, g \in \mathcal{A}$ satifying $f \neq g$ and $f(z) = g(z)$. For such f and g we have $z \in S(f,g)$. As a consequence, we obtain

$$\mathbb{C} = \bigcup \{ S(f,g) : f, g \in \mathcal{A},\ f \neq g \} \tag{1}$$

for every uncountable $\mathcal{A} \subset \mathcal{H}$ with property P_0.

If there is an uncountable set with property P_0, then there must be one with cardinality $\aleph_1$, since every subset of a set with P_0 also has P_0. So let $\mathcal{A}$ is a set of cardinality $\aleph_1$ which has P_0. Then (1) yields

$$|\mathbb{C}| = \left| \bigcup \{ S(f,g) : f, g \in \mathcal{A},\ f \neq g \} \right| \leq |\mathcal{A}| \cdot \aleph_0 = \aleph_1$$

so that CH holds.

[*1] A resort to recursion theoretic argument reveals that the statement Φ is Σ^1_1 in parameters. This observation however does not turn our proof easier.

Recall the Mansfield-Solovay Theorem: *Let* $A \subset \mathbb{R}$ *be* Σ^1_2 *in* $r \subset \omega$. *Then either* A *contains a perfect subset or else* $A \subset L[r]$. Since our $\mathbf{\Sigma}^1_2$ set $\mathcal{A}$ has property P_0, it does not contain a perfect subset. So $\mathcal{A} \subset L[r]$. On the other hand, we also have (1) because $\mathcal{A}$ is uncountable. From this it follows that every $z \in \mathbb{C}$ belongs to the set $S(f, g)$ for some pair f, g of distinct functions in $L[r]$. But then $S(f, g)$ is a countable set arithmetically definable from a pair of "reals" in $L[r]$. Again by the Mansfield-Solovay theorem we have $S(f, g) \subset L[r]$ and $z \in L[r]$. This is our proof of Theorem 2.

3 Proof of Theorem 3

In this section we prove Theorem 3 by applying Arnie Miller's trick (see [2]) to Erdős' construction of uncountable set with property P_0. This means we have now to review the "if" part of Erdős' argument, which is much more tedious than the other part.

Assume CH. The complex numbers are well-ordered into order type ω_1:

$$\mathbb{C} = \{ z_0, z_1, \ldots, z_\alpha, \ldots \} \qquad (\alpha < \omega_1).$$

Fix a countable dense set $D \subset \mathbb{C}$ and enumerate its members as

$$D = \{ d_0, d_1, \ldots, d_k, \ldots \}.$$

By transifinite induction we are going to choose functions $f_\alpha \in \mathcal{H}$ such that

$$\beta < \alpha \ \rightarrow \ f_\beta(z_\beta) \neq f_\alpha(z_\beta) \wedge f_\alpha(z_\beta) \in D. \tag{2}$$

Then all f_α are distinct and for every $\beta < \omega_1$ we have

$$\{ f_\alpha(z_\beta) \, : \, \alpha < \omega_1 \} \subset \{ f_\alpha(z_\beta) \, : \, \alpha \leq \beta \} \cup D.$$

Put then $\mathcal{A} = \{ f_\alpha \, : \, \alpha < \omega_1 \}$. This will be an uncountable set which has property P_0.

Let us explain how we can choose such f_α that meets the requirement (2). Suppose we have already given f_β for $\beta < \alpha$. Re-order α into order type ω:

$$\alpha = \{ \beta_0, \beta_1, \ldots, \beta_n, \ldots \}.$$

Our function $f_\alpha(z)$ will have the form

$$\begin{aligned} f_\alpha(z) &= a_0 + a_1(z - z_{\beta_0}) + a_2(z - z_{\beta_0})(z - z_{\beta_1}) + \cdots \\ &= \sum_{n=0}^{\infty} \left(a_n \cdot \prod_{0 \leq j < n} (z - z_{\beta_j}) \right). \end{aligned} \tag{3}$$

From this we have

$$\begin{aligned} f_\alpha(z_{\beta_0}) &= a_0, \\ f_\alpha(z_{\beta_1}) &= a_0 + a_1(z_{\beta_1} - z_{\beta_0}), \\ &\vdots \end{aligned}$$

and further choice of a_2, a_3, etc. does not affect the values $f_\alpha(z_{\beta_0})$ and $f_\alpha(z_{\beta_1})$. So we can successively choose a_0, a_1, a_2, ... so that

$$\begin{gathered} f_{\beta_0}(z_{\beta_0}) \neq a_0 \in D, \\ f_{\beta_1}(z_{\beta_1}) \neq a_0 + a_1(z_{\beta_1} - z_{\beta_0}) \in D, \\ f_{\beta_2}(z_{\beta_2}) \neq a_0 + a_1(z_{\beta_2} - z_{\beta_0}) + a_2(z_{\beta_2} - z_{\beta_0})(z_{\beta_2} - z_{\beta_1}) \in D, \\ \vdots \end{gathered}$$

in order to meet the requirement (2).

Along with choosing a_n in such a way, we have to take care of magnitude of a_n in order that the series (3) converges and gives a holomorphic function of z.

Let $S^n_j(X_0, \ldots, X_{n-1})$ (where $0 \leq j \leq n < \omega$) denote the elementary symmetric polynomial of order j in n variables $X_0, \ldots, X_{n-1}$ (for $j = 0$, just put $S^n_0 \equiv 1$.) If $d \in \mathbb{C}$ we have

$$\prod_{0 \leq j < n} (z - z_{\beta_j}) = \sum_{j=0}^{n} S^n_j(d - z_{\beta_0}, \ldots, d - z_{\beta_{n-1}})(z - d)^{n-j}. \tag{4}$$

So if we put for each $n \in \omega$

$$R_n = \max\{\, |S^n_j(d_k - z_{\beta_0}, \ldots, d_k - z_{\beta_{n-1}})| \;:\; k, j \leq n \,\} \tag{5}$$

(recall that $D = \{\, d_k : k \in \omega \,\}$ is a countable dense subset of $\mathbb{C}$), $n \geq k$ and $|z - d_k| \leq 1/2$ implies

$$\begin{aligned} \left| \prod_{0 \leq j < n} (z - z_{\beta_j}) \right| &\leq \sum_{j=0}^{n} \left| S^n_j(d_k - z_{\beta_0}, \ldots, d_k - z_{\beta_{n-1}})(z - d_k)^{n-j} \right| \\ &\leq R_n \cdot \sum_{j=0}^{n} 2^{-(n-j)} \\ &\leq 2R_n. \end{aligned} \tag{6}$$

From this it follows that if we choose a_n so that

$$|a_n| \leq \frac{1}{2^n R_n}, \tag{7}$$

then under the condition $|z - d_k| \leq 1/2$, we have

$$\sum_{n=k}^{\infty} \left| a_n \cdot \prod_{0 \leq j < n} (z - z_{\beta_j}) \right| \leq \sum_{n=k}^{\infty} 2^{-n+1} = 2^{-k+2}$$

by (6) and (7). So the series (3) converges uniformly on the closed disk

$$\bar{D}(d_k; \tfrac{1}{2}) = \{\, z \,:\, |z - d_k| \leq 1/2 \,\}$$

for every $k \in \omega$. But since $D = \{\, d_k : k \in \omega \,\}$ is dense every $z \in \mathbb{C}$ has a neighborhood of the form

$$D(d_k; \tfrac{1}{2}) = \{\, z \,:\, |z - d_k| < 1/2 \,\}.$$

That is to say, the series (3) converges uniformly on a neighborhood of each z. Therefore the sum $f_\alpha(z)$ is a holomorphic function of z. This completes Erdős' proof that CH implies existence of an uncountable set with property P_0.

Suppose now that $\mathbb{R}$, and hence also $\mathbb{C}$ are contained in $L[r]$ with some $r \subset \omega$. We are to explain how we can find such $\mathcal{A}$ among $\mathbf{\Pi}^1_1$ sets. In order to simplify notation, let us assume $r = \emptyset$ and suppress mentioning it.

We know the wellordering relation $<_L$ of L restricted to $\mathbb{C}$ has order type ω_1. So we may assume our wellordering

$$\mathbb{C} = \{ z_0, z_1, \ldots, z_\alpha, \ldots \} \qquad (\alpha < \omega_1)$$

agrees with $<_L$. Assume also the enumeration of our countable dense set

$$D = \{ d_0, d_1, \ldots, d_n, \ldots \}$$

is arithmetically definable. Let us also choose the re-ordering

$$\alpha = \{ \beta_0, \beta_1, \ldots, \beta_n, \ldots \}$$

to be the $<_L$-minimum such enumeration. Under these conditions we construct f_α just as Erdős did but with one extra tweek.

Note that when we choose a_n which meet the requirements (2) and (7), we still have infinitely many possibility of the value of a_n that suits. Using this freedom of choice, we can let the function f_α code a prescribed infinite sequence of zeros and ones. It follows that *our f_α can code any prescribed countable set of information.*

We let f_α code *all ingredients of our construction of itself:* the ordinal α, its enumeration $\langle \beta_n : n \in \omega \rangle$, the sequence of numbers $\langle z_\beta : \beta \leq \alpha \rangle$, previously chosen functions $\langle f_\beta : \beta < \alpha \rangle$, and so on. Then it follows that f_α "knows" how it has been constructed. We also make sure that f_α is the $<_L$-minimum function which meets all these conditions we have put so far. Then a function $f \in \mathcal{H}$ is one of such f_α if and only if there are parameters in $L_{\omega_1^{\mathrm{CK}}(f)}[f]$ (the smallest admissible set containing f) which define f in such and such way and f is the $<_L$-minimum function in $L_{\omega_1^{\mathrm{CK}}(f)}[f]$ which meet such and such conditions. As long as the "such and such" parts are written aritmetically, this gives a Π^1_1 description of the set $\{ f_\alpha : \alpha < \omega_1 \}$ because the equivalence gives a Σ_1 formula $\psi(v)$ such that

$$\exists \alpha < \omega_1 (f = f_\alpha) \leftrightarrow L_{\omega_1^{\mathrm{CK}}}[f] \models \psi(f).$$

It follows that the set $\mathcal{A} = \{ f_\alpha : \alpha < \omega_1 \}$ is an uncountable $\mathbf{\Pi}^1_1$ set which have property P_0.

References

[1] P. Erdős, *An interpolation problem associated with the continuum hypothesis*, Michigan Math. J. **11** (1964), 9–10

[2] A.W. Miller, *Infinite Combinatorics and Definability*, Ann. Pure Appl. Logic **41-2** (1989), 179–203.

[3] Y.N. Moschovakis, **Descriptive Set Theory** (Second Edition), American Mathematical Society 2009.

[4] W. Rudin, **Real and Complex Analysis** (Third International Edition), McGraw-Hill 1987.