# *Matematické struktury* lecture/tutorial on February 20, 2017: corollaries of the axiom of choice

Martin Klazar[*]

February 21, 2017

The *axiom of choice* or *AC* ("axiom výběru" in Czech) says that for any surjection $f:\ A \to B$ there is a mapping $g:\ B \to A$ such that $f \circ g:\ B \to B$ is an identity on $B$. In other words, for every set system $(M_i \mid i \in I)$ of nonempty sets there is a selector map $g:\ I \to \bigcup_{i \in I} M_i$ with the property that $g(i) \in M_i$ for every $i \in I$. Yet equivalently, for every set $S$ with $\emptyset \not\in S$ there is a selector map $g:\ S \to \bigcup S$ such that $g(s) \in s$ for every $s \in S$.

We would like to have a function $\mu:\ \exp(C) \to \mathbb{R}_{\ge 0}$ assigning to any subset of the unit circle

$$C = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

a nonnegative real number so that

1. $\mu(C) = 2\pi = 6.282\dots;$
2. if $A_1, A_2, \ldots \subset C$ is a finite or infinite sequence of pairwise disjoint sets then $\mu(A_1 \cup A_2 \cup \ldots) = \mu(A_1) + \mu(A_2) + \ldots$; and
3. for every $A \subset C$ and every rotation $\varphi_\alpha$ of $C$, $\alpha \in [0, 2\pi)$, counter-clockwise by the angle $\alpha$ around the origin we have $\mu(\varphi_\alpha(A)) = \mu(A)$.

Here, for $a = (a_x, a_y) \in C$ and $A \subset C$, we have

$$\varphi_\alpha(a) = (a_x \cos\alpha - a_y \sin\alpha,\ a_x \sin\alpha + a_y \cos\alpha)$$

and $\varphi_\alpha(A) = \{\varphi_\alpha(a) \mid a \in A\}$. Note that if one of $\alpha$ or $x$ is fixed then the univariate map $\varphi_\alpha(x)$ is injective. Thus $\mu$ should assign to $C$ the familiar length, should be countably additive, and should be preserved under rotations. The usual arc-length on $C$ we work with in mathematical practice has all these properties.

However, we show that AC implies that no such function $\mu$ exists. We call an angle $\alpha \in [0, 2\pi)$ *rational* if $\alpha/\pi \in \mathbb{Q}$ and denote by $\mathcal{R}$ the set of all rational angles.

[*] `klazar@kam.mff.cuni.cz`

**Theorem 1 (Vitali, 1905)** *By AC, no function $\mu:\ \exp(C)\to\mathbb{R}_{\ge 0}$ has properties 1–3.*

*Proof.* The properties required from $\mu$ are contradictory because there exists a set $X\subset C$ such that

$$\{\varphi_\alpha(X)\mid \alpha\in\mathcal{R}\}$$

is a set partition of $C$: the union of these (nonempty) sets equals $C$ and they are pairwise disjoint. Then

$$2\pi=\mu(C)=\mu(\textstyle\bigcup_{\alpha\in\mathcal{R}}\varphi_\alpha(X))=\sum_{\alpha\in\mathcal{R}}\mu(\varphi_\alpha(X))=\sum_{\alpha\in\mathcal{R}}\mu(X)=0,\ +\infty$$

— a contradiction. The first equality is by property 1 of $\mu$, the second and third follow from property 2 and the fact that the above sets partition $C$, the fourth follows from property 3, and the last equality (trivial infinite series summation) reads $=0$ for $\mu(X)=0$ and $=+\infty$ for $\mu(X)>0$. In either case it does not equal $2\pi$.

To obtain $X$, we consider a binary relation $\sim$ on $C$, $a\sim b$ if and only if $a=\varphi_\alpha(b)$ for some $\alpha\in\mathcal{R}$. It is an equivalence: $a=\varphi_0(a)$ proves reflexivity, $a=\varphi_\alpha(b)\rightsquigarrow\varphi_{2\pi-\alpha}(a)=b$ proves symmetry, and $a=\varphi_\alpha(b),b=\varphi_\beta(c)\rightsquigarrow a=\varphi_{\alpha+\beta}(c)$ ($\alpha+\beta$ is taken modulo $2\pi$) proves transitivity. We apply AC on the set

$$C/{\sim}=\{[a]\mid a\in C\}$$

of equivalence classes, called blocks, that $\sim$ partitions $C$ into. A block is the set $[a]=\{b\in C\mid a\sim b\}$. From each block we select exactly one element and collect them in the set $X\subset C$. We show that $X$ has the stated property. If $a\in C$ is arbitrary then $a=\varphi_\alpha(x)$ for some $\alpha\in\mathcal{R}$ for the $x\in[a]\cap X$, thus rational rotations of $X$ cover the whole $C$. If $a\in\varphi_\alpha(X)\cap\varphi_\beta(X)$ for some $\alpha,\beta\in\mathcal{R}$ with $\alpha<\beta$, then $a=\varphi_\alpha(x)=\varphi_\beta(y)$ for two distinct $x,y\in X$, so $x=\varphi_{\beta-\alpha}(y)$ and $x\sim y$. This is impossible because the elements of $X$ are pairwise unrelated by $\sim$. Thus for different $\alpha\in\mathcal{R}$ the sets $\varphi_\alpha(X)$ do not intersect. □

The above displayed computation shows that $X$ cannot be assigned any length and this subset of $C$ is *non-measurable.* We will use it later for a paradoxical decomposition of $C$. The theorem does not say that to define a reasonable notion of arc-length on $C$ is an impossible task (as we know, it can be accomplished in a quite satisfactory manner), it only shows that we have to leave $\mu$ undefined on some wild subsets of $C$.

We explain the second paradox following from AC. We let

$$M=\{f:\ \mathbb{R}\to\mathbb{R}\}=\mathbb{R}^{\mathbb{R}}$$

be the set of all real functions defined on the real numbers. For $f\in M$ and $a\in\mathbb{R}$ we denote by $f\,|\,a$ the restriction $f\,|\,(-\infty,a)$. An *oracle* is a map

$$V:\ \{g:\ (-\infty,a)\to\mathbb{R}\mid a\in\mathbb{R}\}\to\mathbb{R}$$

that assigns a real number to any real function defined on the real numbers smaller than some $a \in \mathbb{R}$. $V$ *guesses correctly the value* $f(a)$, for $f \in M$ and $a \in \mathbb{R}$, if

$$V(f \,|\, a) = f(a) \ ,$$

and else $V$ *errs at* $f(a)$. Thus oracle attempts to guess the value of $f$ at $a$ only on the basis of the values $f(x)$ with $x < a$.

For example, it is easy to define an oracle for the class of functions $C(\mathbb{R})$ in place of $M$, i.e. for all continuous functions from $\mathbb{R}$ to $\mathbb{R}$. We define

$$V:\ \{g:\ (-\infty, a) \to \mathbb{R} \mid a \in \mathbb{R},\ \lim_{x \to a-0} g(x) \in \mathbb{R}\} \to \mathbb{R}$$

by setting $V(g)$ to be the value of the mentioned limit. Then $V(f \,|\, a) = f(a)$ for every $a \in \mathbb{R}$ and every $f \in C(\mathbb{R})$ by continuity of $f$ at $a$, and so this oracle guesses correctly every value of every continuous function. Of course, this is almost a triviality. For another example, or rather a non-example, of an oracle consider the class of functions

$$N = \{f:\ \mathbb{N} \to \mathbb{R}\} = \mathbb{R}^{\mathbb{N}}$$

where $\mathbb{N} = \{1, 2, \dots\}$ are the natural numbers. Now it is easy to see that for every candidate oracle

$$V:\ \{g:\ [n-1] \to \mathbb{R} \mid n \in \mathbb{N}\} \to \mathbb{R}$$

that assigns a real number to any real function defined on an initial segment $[n-1] = \{1, 2, \dots, n-1\}$ of the natural numbers (for $n = 1$ there is just one such function, $g = \emptyset$), there is a function $f \in N$ such that

$$V(f \,|\, n) = V(f \,|\, [n-1]) \neq f(n)$$

for every $n \in \mathbb{N}$ — $V$ errs at every value of $f$. Just set inductively

$$f(n) := V(f \,|\, n) + 1,\ \ n \in \mathbb{N}\ ,$$

say (recall that $f \,|\, n = f \,|\, [n-1]$ and that $f \,|\, 1 = \emptyset$ where the inductive definition of $f$ starts).

For the classes of functions $C(\mathbb{R})$ and $N$ we have answered the question for an oracle easily, the former class has a trivial oracle that guesses correctly every value of every function and for the latter class every oracle has to err at every value of some function. What can be said in the original setting for the class $M$ of all real functions?

**Theorem 2 (Hardin and Taylor, 2008)** *By AC, there is an oracle $V$ that for every $f \in M$ correctly guesses almost every value $f(a)$, with at most countably many exceptions $a \in \mathbb{R}$.*

At least to me, this is quite a counterintuitive result. One may interpret it as a refutation of free will: if one builds a function $f:\ \mathbb{R} \to \mathbb{R}$ step by step by moving $a \in \mathbb{R}$ from $-\infty$ to $+\infty$, then except for at most countably many flashes of free will, at almost all instances $a$ (recall that $\mathbb{R}$ is uncountable) the value $f(a)$ is predetermined by the earlier values $f(x)$ with $x < a$ and one has no choice! For the proof we need yet another (fourth) formulation of the axiom of choice:

> Every set $A$ can be well-ordered, there is a linear ordering $\leq$ on $A$ such that every nonempty subset $B \subset A$ has a least element, a unique element $b \in B$ satisfying $b \leq c$ for every $c \in B$ which we denote $\min_{\leq}(B)$ .

*Proof.* We invoke the axiom of choice and linearly well-order $M$ by $\preceq$. For $a \in \mathbb{R}$ and $g:\ (-\infty, a) \to \mathbb{R}$ we define our miraculous oracle by

$$V(g) = f_0(a) \ \text{ where } \ f_0 = \min_{\preceq}(\{f \in M \mid f\,|\,a = g\}) \ .$$

We show that $V$ has the stated property. For an arbitrary $f \in M$ we take the set

$$X = \{a \in \mathbb{R} \mid V(f\,|\,a) \neq f(a)\}$$

of arguments where $V$ errs and show that it is well-ordered in the standard linear ordering $(\mathbb{R}, \leq)$ of the real numbers. Since every well-ordered subset in $(\mathbb{R}, \leq)$ is at most countable (finite or infinite countable), as we prove at the end, we are done.

For our $f$ and $a \in \mathbb{R}$, let $A_a = \{g \in M \mid g\,|\,a = f\,|\,a\}$ and $f_a = \min_{\preceq}(A_a)$, so $V(f\,|\,a) = f_a(a)$ by the definition of $V$. If $a, b \in \mathbb{R}$ with $a < b$ then $f_a \preceq f_b$ because $A_a \supset A_b$. Now if $a \in X, b \in \mathbb{R}$ with $a < b$ then even $f_a \prec f_b$ because

$$f_a(a) = V(f\,|\,a) \neq f(a) = (f\,|\,b)(a) = f_b(a)$$

shows that $f_a \neq f_b$. If $X$ were not well-ordered in $(\mathbb{R}, \leq)$ it would contain an infinite descending chain $a_1 > a_2 > \dots$ . By the previous result this would give an infinite descending chain $f_{a_1} \succ f_{a_2} \succ \dots$ in $(M, \preceq)$, which is impossible by the well-ordering of $M$. So $X$ is well-ordered by $\leq$.

It remains to prove that every (nonempty) subset $Y \subset \mathbb{R}$, well-ordered by $\leq$, is at most countable. We produce an injection $z:\ Y \to \mathbb{Q}$. For $a \in Y$ we set

$$z(a) = \text{ some } \alpha \in \mathbb{Q} \cap (a, \min_{\leq}(\{b \in Y \mid b > a\})) \ .$$

If $a$ happens to be the maximum of $Y$, we define the minimum as $+\infty$. Thus $z(a)$ is a fraction in the gap between $a$ and the successor of $a$ in $Y$, or a fraction after $a$ if $a$ has in $Y$ no successor. It is immediate from the definition that $z(a) \neq z(b)$ for $a < b$ in $Y$. $\mathbb{Q}$ is countable, so $Y$ is also countable or finite. □

We return to the set $X \subset C$ whose rational rotations partition the unit circle $C$. In the next lecture I will prove the following result and mention related paradoxes and relevant literature.

**Proposition 3** *Let $D$ be a (disjoint) copy of $C$, for example $D = \{(x, y) \in \mathbb{R}^2 \mid (x-3)^2 + y^2 = 1\}$. Under the axiom of choice there exist a partition*

$$C = \bigcup_{n=1}^{\infty} A_n \quad \textit{and rigid motions} \quad \psi_n : \mathbb{R}^2 \to \mathbb{R}^2$$

*such that $\psi_n(A_n)$ form the partition*

$$C \cup D = \bigcup_{n=1}^{\infty} \psi_n(A_n) \ .$$

"Rigid motion" is a translation combined with a rotation (around a point). The proposition thus states that under the assumption of AC there exists a puzzle with countably many pieces which one can assemble in one way in the unit circle $C$ and in another way (after moving the pieces in the plane without deformations and changes in size) in two disjoint copies of $C$. Something from nothing is created! Try to prove Proposition 3 by yourself, it is not hard.