MATHEMATICAL STRUCTURES (NMAI064)
summer term 2024/25
lecturer: Martin Klazar

LECTURE 10 (April 23, 2025)
AXIOM OF CHOICE AND ITS CONSEQUENCES: NON-MEASURABLE SETS, THE WELL ORDERING THEOREM, THE PROPHET PARADOX

• *The Axiom of Choice (*AC*)* is the set-theoretic axiom that

$$\forall\, A\colon\ \emptyset \not\in A \Rightarrow \exists\, F\colon\ (F\colon A \to \bigcup A) \wedge (B \in A \Rightarrow F(B) \in B)\ .$$

As you certainly know, the *sum* $\bigcup A$ *of* A, is the set $\bigcup A$ such that $B \in \bigcup A \iff \exists\, C \in A\colon\ B \in C$. The notation $F\colon A \to B$, i.e., F is a *function (map) from* A *to* B, abbreviates the fact that F is a set of ordered pairs (C, D) such that always $C \in A$, $D \in B$, and for every $C \in A$ there exists exactly one $D \in B$ with $(C, D) \in F$.

Exercise 1 *Show that the* AC *is equivalent with the claim that for every surjection* $F\colon A \to B$ *there is a map* $G\colon B \to A$ *such that*

$$F(G) = F \circ G = \mathrm{id}_B\,.$$

Exercise 2 *Show that the* AC *is equivalent with the claim that for every set system* $\{A_i\colon\ i \in I\}$, $A_i \neq \emptyset$, *there is a map*

$$F\colon I \to \textstyle\bigcup_{i\in I} A_i$$

such that $F(i) \in A_i$ *for every* $i \in I$.

• *Equivalences and partitions.* First let us review equivalence relations and set partitions. $R \subseteq A \times A$ *is an equivalence relation* on A if it is

- reflexive $-$ $\forall\, a \in A\colon\ aRa$,
- symmetric $-$ $\forall\, a, b \in A\colon\ aRb \Rightarrow bRa$, and
- transitive $-$ $\forall\, a, b, c \in A\colon\ aRb \wedge bRc \Rightarrow aRc$

A set *partition* of a set A is a set B such that $\emptyset \not\in B$, the elements of B are mutually disjoint and $\bigcup B = A$. For any equivalence relation R on a set A we define the *blocks of* R to be the sets

$$[a]_R = \{b \in A\colon\ aRb\},\ a \in A\,.$$

Exercise 3 *For every set A and every equivalence relation R on A,*

$$A/R := \{[a]_R\colon\ a \in A\}$$

is a partition of A.

Exercise 4 *For every set A and every partition P of A,*

$$R(P) := \{(a,\, b) \in A^2\colon\ \exists\, B \in P\colon\ a,\, b \in B\}$$

is an equivalence relation on A.

Exercise 5 *For every set A, every equivalence relation S on A and every partition P of A,*

$$R(A/S) = S \ \text{ and } \ A/R(P) = P\,.$$

Exercise 6 *For $n \in \mathbb{N} = \{1, 2, \dots\}$ let B_n, the* Bell number[1], *be the number of equivalence relations on an n-element set X. Why does B_n depend only on the cardinality of X and not on the elements of X? Prove that for every n,*

$$B_n < B_{n+1}\ .$$

• *Non-measurable sets.* Let

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

be the *unit circle* in the Euclidean plane $\mathbb{R}^2$. For any angle $\varphi \in [0, 2\pi)$ we denote by

$$F_\varphi\colon S \to S,\quad (x,\, y) \mapsto (?_x,\, ?_y)\ ,$$

the *counter-clockwise rotation around the origin by the angle φ*. It is clearly a bijection. An angle $\varphi \in [0, 2\pi)$ is *rational* if $\frac{\varphi}{\pi} \in \mathbb{Q}$. We denote the set of rational angles by $[0, 2\pi)_{\mathbb{Q}}$. Obviously, $[0, 2\pi)_{\mathbb{Q}}$ is a countable set.

Exercise 7 *Define the additive Abelian group*

$$([0,\, 2\pi)_{\mathbb{Q}},\, +)$$

of addition modulo 2π. Find the above formulas $?_x$ and $?_y$ in the definition of F_φ and show that for any $\varphi, \varphi' \in [0, 2\pi)_{\mathbb{Q}}$,

$$F_\varphi \circ F_{\varphi'} = F_{\varphi+\varphi'}\ .$$

[1]Named after Eric T. Bell (1883–1960).

Show that for any fixed $x \in S$, the function $F_\varphi(x)$ is injective in the variable $\varphi \in [0, 2\pi)$.

For the unit circle S we denote by $\mathcal{P}(S)$ the set of subsets of S. For a subset $X \subseteq \mathcal{P}(S)$ with $S \in X$, we say that a map

$$\lambda \colon X \to [0, +\infty)$$

is an *arc length on* X if the following three conditions hold.

1. $\lambda(S) > 0$ — the whole unit circle has positive arc length.
2. For every pairwise disjoint sets $A_n \in X$, $n \in \mathbb{N}$, with $\bigcup_{n=1}^{\infty} A_n \in X$ one has that
$$\lambda(\textstyle\bigcup_{n=1}^{\infty} A_n) = \sum_{n=1}^{\infty} \lambda(A_n)\,.$$
We say that the arc length is σ-additive.
3. For every $\varphi \in [0, 2\pi)$ and every $A \in X$, if $F_\varphi[A] \in X$ then
$$\lambda(F_\varphi[A]) = \lambda(A)\,.$$
We say that the arc length is invariant under rotations.

Theorem 8 (a troublesome set) *There exists a set $X \subseteq S$ such that the set*

$$\{F_\varphi[X] \colon \ \varphi \in [0, 2\pi)_{\mathbb{Q}}\}$$

is a partition of S.

Proof. By Exercise 9, the relation $\sim$ on S, defined by

$$a \sim b \iff \exists\, \varphi \in [0,\, 2\pi)_{\mathbb{Q}} \colon \ F_\varphi(a) = b\ ,$$

is an equivalence relation. We define $X \subseteq S$ by means of the AC by taking one representative element from each block of $\sim$. We show that for φ running in $[0, 2\pi)_{\mathbb{Q}}$ the sets $F_\varphi[X]$ are disjoint and form a partition of S. Their union is S because each $s \in S$ lies in a block B of $\sim$ and thus $F_\varphi(r) = s$ for some $\varphi \in [0, 2\pi)_{\mathbb{Q}}$ for the representative $r \in X$ of B. If $F_\varphi[X] \cap F_{\varphi'}[X] \neq \emptyset$ for two distinct rational angles φ and φ', then

$$F_\varphi(r) = F_{\varphi'}(r') \ \text{ for some } \ r, r' \in X\ .$$

Then $r \neq r'$ by the injectivity of $F_\varphi(x)$ in φ for fixed x (Exercise 7). Also,

$$F_{\varphi-\varphi'}(r) = r' \ \text{ for } \ \varphi - \varphi' \in [0,\, 2\pi)_{\mathbb{Q}}$$

(again by Exercise 7) and therefore $r \sim r'$. This is impossible for two distinct elements of X. It is clear that always $F_\varphi[X] \neq \emptyset$. $\square$

Exercise 9 *Prove that the relation $\sim$ on S defined in the previous proof is an equivalence relation.*

Corollary 10 (impossible arc length) *There is no arc length λ on the whole power set $\mathcal{P}(S)$.*

Proof. Indeed, suppose in the way of contradiction that

$$\lambda\colon \mathcal{P}(S) \to [0,\, +\infty)$$

is an arc length and consider the set $X \subseteq S$ of the previous theorem. Then we get by the theorem and by the three properties of any arc length that

$$\lambda(S) = \textstyle\sum_{\varphi\in[0,\,2\pi)_{\mathbb{Q}}} \lambda(F_\varphi[X]) = \sum_{\varphi\in[0,\,2\pi)_{\mathbb{Q}}} \lambda(X) = 0 \ \text{ or } \ +\infty\,.$$

But this is a contradiction because $\lambda(S) \in (0, +\infty)$. $\square$

Exercise 11 *Show that if* property 1 *of arc length is not required, then the previous corollary does not hold.*

- *Well orderings.* Let X be a set. A relation

$$\leq_X \subseteq X^2$$

is a *linear order* on X if it is reflexive, transitive, weakly asymmetric ($a \leq_X b \wedge b \leq_X a \Rightarrow a = b$) and total ($\forall\, a, b \in X\colon\ a \leq_X b \vee b \leq_X a$). We say that a linear order $\leq_X$ on X is a *well ordering* if every nonempty set $Y \subseteq X$ has a minimum element $y \in Y$: for every $z \in Y$ we have $y \leq_X z$.

Exercise 12 *Prove that minimum elements are unique.*

Exercise 13 *A linear order $(X, \leq_X)$ is a well ordering if and only if there is no infinite strictly descending chain*

$$x_1 >_X x_2 >_X \ldots,\ \ x_n \in X\,.$$

Here $x >_X y$ means that $y \leq_X x$ and $y \neq x$.

Exercise 14 *Assume that there is a well ordering on every set and deduce from this the* AC.

Theorem 15 (Zermelo) *The axiom of choice holds if and only if every set has a well ordering.*

Proof. The "if" part is proven in Exercise 14. We prove the other implication: if AC holds then every set has a well ordering. Let $X \neq \emptyset$ and $f\colon \mathcal{P}(X) \setminus \{\emptyset\} \to X$ be a *selector on* X, i.e., a function satisfying $f(A) \in A$ (it is guaranteed by AC). We consider the set

$$L = \{R\colon\ R \subseteq D(R)^2,\ D(R) \subseteq X,\ R \text{ is a linear order on } D(R)\}$$

of linear orders R on sets $D(R) \subseteq X$. For any $R \in L$ we set

$$D_R = \{A \subseteq D(R)\colon\ x, y \in D(R),\ y \in A,\ xRy \Rightarrow x \in A\}\,.$$

So D_R is the set of *downsets* in the linear order R. Let further

$$C = \{R \in L\colon\ A \in D_R,\ A \neq D(R) \Rightarrow f(X \setminus A) = \min_R(D(R) \setminus A)\}$$

be those linear orders R on subsets $D(R)$ of X, for which for every proper downset A in R the selector f chooses from its complement to X an element that is also the minimum element of the complement of A to $D(R)$. We show that C contains (as an element) a well ordering on X. The set $C \neq \emptyset$, for example $\{(f(X), f(X))\} \in C$.

Firstly we show that every $R \in C$ is a well ordering on $D(R)$. Let $R \in C$. For any nonempty $B \subseteq D(R)$ we set

$$A = \{y \in D(R) \setminus B\colon\ x \in B \Rightarrow yRx\}\,.$$

The set $D(R) \setminus A$ contains B and is therefore nonempty. Clearly, A is a downset in R. Thus

$$y = f(X \setminus A) = \min_R(D(R) \setminus A)\,.$$

From the facts that $D(R) \setminus A \supset B$ and that y is the minimum element in $D(R) \setminus A$ we get that yRx for every $x \in B$. If $y \notin B$, we would have $y \in A$ by the definition of A, which is impossible. Hence y is in B and is the minimum element of B, even of the superset $D(R) \setminus A$.

Secondly we show that for every two linear orders $R, S \in C$ one of them extends the other: $D(R) \in D_S \wedge R \subseteq S$ or $D(S) \in D_R \wedge S \subseteq R$. Let $R, S \in C$ be given; we set

$$A = \{x \in D(R) \cap D(S) \mid Rx = Sx \wedge R \cap (Rx \times Rx) = S \cap (Sx \times Sx)\}$$

(here $Rx = \{y \in D(R) \mid yRx\}$ and similarly for Sx). The set A consists exactly of the elements that determine the same downset in R and in S, that is moreover ordered in R and in S in the same way. We claim that $A \in D_R \cap D_S$ — A is a downset both in R and in S). Let

$$z,\ y,\ x \in X \ \text{ with } \ x \in A \ \text{ and } \ yRx\ .$$

Then ySx because $Rx = Sx$. If zRy then zSy and vice-versa (in both cases $y, z \in Rx = Sx$ and this set is ordered in the same way in R and in S). Thus $Ry = Sy$. This set is contained in $Rx = Sx$, and therefore it is ordered in the same way both in R and in S. Hence $y \in A$ and A is a downset in R. One shows in the same way that A is a downset in S.

Now if both $D(R) \setminus A$ and $D(S) \setminus A$ are nonempty, $y = f(X \setminus A)$ is the minimum element of $D(R) \setminus A$ with respect to R and it is also the minimum element of $D(S) \setminus A$ with respect to S, and so $Ry = A \cup \{y\} = Sy$. It is also clear that R and S give $A \cup \{y\}$ the same order (they add a new element y at the end), and so $y \in A$, which is a contradiction. Thus for example $A = D(R)$, $R \subseteq S$ and S extends R.

Thirdly we show that

$$T = \bigcup C \in C\,,$$

and therefore C has (unique) inclusion-wise maximum element. By the previous paragraph, T is a linear order on $D(T) = \bigcup_{R \in C} D(R)$ and for $x, y \in D(T)$ we have xTy, if and only if xRy for some $R \in C$ with $x, y \in D(R)$. We check that T has the property defining C. Let $A \subseteq D(T)$ be a proper downset in T and let $b \in D(T) \setminus A$ be arbitrary. Thus $b \in D(R)$ for some $R \in C$. We show that $A \subseteq D(R)$. If $a \in A$ is arbitrary, then $a \in D(S)$ for some $S \in C$. If $D(S) \in D_R$, then $a \in D(R)$. If $D(R) \in D_S$ and aSb, then again $a \in D(R)$. The case bSa does not occur (for then one would have $b \in A$). Hence

$A \subseteq D(R)$ and $D(R) \setminus A \neq \emptyset$. Therefore the element $y = f(X \setminus A)$ is the minimum element in $D(R) \setminus A$ and yRb. Since b was arbitrary, y is the minimum element in $D(T) \setminus A$ and we see that $T \in C$.

In conclusion we show that $D(T) = X$, and T is therefore the sought-for well ordering of X. If $D(T) \neq X$, then we could extend T by the element $x := f(X \setminus D(T))$ to R:

$$D(R) := D(T) \cup \{x\} \text{ and } yRx \text{ for every } y \in D(R) \tag{1}$$

— we add to T a new maximum element. It is clear that $R \in C$ (Exercise 16). Since R properly extends T, we have a contradiction with the maximality of T. □

The previous proof is taken from a manuscript of A. Pultr.

Exercise 16 *Show that the linear order R defined in equation* (1) *indeed belongs to C.*

• *The prophet paradox.* Let $(X, \leq_X)$ be a linear order. For any $a \in X$ and any map $f \colon X \to Y$ we denote by $f_{|a}$ the restriction of f to the set

$$\{b \in X \colon\ b <_X a\} .$$

For a linear order $(X, \leq_X)$ and a family $\mathcal{F}$ of functions $f \colon X \to Y$, an $(X, \mathcal{F})$-*prophet* is a map

$$P \colon \{f_{|a} \colon\ f \in \mathcal{F},\ a \in X\} \to Y .$$

The value $P(f_{|a}) \in Y$ is the guess of P for the value $f(a)$. The prophet tries to guess from the values $f(b)$ for all $b <_X a$ the value of f at a. If $P(f_{|a}) = f(a)$ then P *succeeds for f at a*, else P *errs for f at a*.

Exercise 17 *Let $(X, \leq_X) = (\mathbb{R}, \leq)$ be the standard linear order of real numbers and let*

$$\mathcal{F} = C(\mathbb{R}) = \{f \colon \mathbb{R} \to \mathbb{R} \colon\ f \textit{ is continuous}\}$$

be the set of continuous real functions defined on $\mathbb{R}$. The exercise is to find an $(\mathbb{R}, C(\mathbb{R}))$-prophet that succeeds for f at a for every $f \in C(\mathbb{R})$ and every $a \in \mathbb{R}$.

On the other hand we have the following equally simple result.

Proposition 18 (all prophets err) *For $n \in \mathbb{N}$, let*

$$(X, \leq_X) = ([n], \leq) = (\{1, 2, \ldots, n\}, \leq)$$

be the usual linear order on the first n natural numbers and let

$$\mathcal{F} = Y^{[n]} = \{\textit{all maps from } [n] \textit{ to } Y\} ,$$

where Y is a set with at least two elements. Then it is true that for every $([n], Y^{[n]})$-prophet P there exists a function $f \in Y^{[n]}$ such that

$$\forall\, a \in [n] :\ P(f_{|a}) \neq f(a) .$$

Thus P errs for f at its every argument $a \in [n]$.

Proof. Let

$$P\colon \{g\colon\ g\colon [m] \to Y,\, m \in \{0, 1, \ldots, n-1\}\} \to Y$$

be an $([n], Y^{[n]})$-prophet. We set $[0] = \emptyset$. We define the values $f(m)$ of the required function $f\colon [n] \to Y$ by induction on $m = 1, 2, \ldots, n$. At the start we take $f(1) \in Y$ so that $f(1) \neq P(\emptyset)$, which is possible as $|Y| \geq 2$. If $m \in [n]$, $m > 1$ and $f(1), f(2), \ldots, f(m-1)$ are already defined, we take

$$f(m) \in Y \setminus \{P(f_{|m})\} .$$

Again, this is possible as $|Y| \geq 2$. It is clear that P errs for the function f at its every argument. □

Exercise 19 *What happens when $|Y| \leq 1$?*

One might think that when in Exercise 17 the family of continuous functions is extended to the family $\mathcal{F} = \mathbb{R}^{\mathbb{R}}$ of all real function, one obtains a result similar to the previous proposition, namely that every prophet has to err for a troublesome function very often. Surprisingly, quite the opposite is the case under the assumption of AC. There exists a prophet that for every real function almost never errs.

Theorem 20 (the prophet paradox) *Let $(X, \leq_X) = (\mathbb{R}, \leq)$ be the usual linear order of real numbers and let*

$$\mathcal{F} = \mathbb{R}^{\mathbb{R}} = \{\textit{all functions from } \mathbb{R} \textit{ to } \mathbb{R}\} .$$

Then there exists an $(\mathbb{R}, \mathbb{R}^{\mathbb{R}})$-prophet P such that

$\forall\, f \in \mathbb{R}^{\mathbb{R}}$: *the set $\{a \in \mathbb{R}\colon\ P$ errs for f at $a\}$ is at most countable .*

Proof. We define P by means of the well ordering

$$(\mathbb{R}^{\mathbb{R}}, \preceq)$$

that exists by Theorem 15 under the assumption of AC. For $g \in \mathbb{R}^{\mathbb{R}}$ and $a \in \mathbb{R}$ we set

$$P(g_{|a}) = g_0(a) \text{ where } g_0 = \min_{\preceq}(\{h \in \mathbb{R}^{\mathbb{R}}\colon\ h_{|a} = g_{|a}\})\,.$$

Now let an $f \in \mathbb{R}^{\mathbb{R}}$ be given. We take the set

$$X = \{a \in \mathbb{R}\colon\ P(f_{|a}) \neq f(a)\}$$

of errors of P for f. Let $a < b$ with $a \in X$ be two real numbers,

$$g_a = \min_{\preceq}(\underbrace{\{g \in \mathbb{R}^{\mathbb{R}}\colon\ g_{|a} = f_{|a}\}}_{M_a}) \text{ and } g_b := \min_{\preceq}(\underbrace{\{g \in \mathbb{R}^{\mathbb{R}}\colon\ g_{|b} = f_{|b}\}}_{M_b})\,.$$

From $a < b$ we get that $M_b \subseteq M_a$ and $g_a \preceq g_b$. From

$$g_a(a) = P(f_{|a}) \neq f(a) = g_b(a)$$

we see that $g_a \neq g_b$. Thus $g_a \prec g_b$. We see that the linear order $(X, \leq)$ (with the usual order $\leq$ of real numbers) is a well ordering. Else, by Exercise 13, we would have in $(X, \leq)$ an infinite strictly descending chain $a_1 > a_2 > \ldots$, which would yield by the last argument an infinite strictly descending chain $g_{a_1} \succ g_{a_2} \succ \ldots$ in $(\mathbb{R}^{\mathbb{R}}, \preceq)$. But the last chain does not exist because $(\mathbb{R}^{\mathbb{R}}, \preceq)$ is a well ordering. Since $(X, \leq)$ is a well ordering, by the next Exercise 21 the set X is at most countable. $\square$

Exercise 21 *Let $(\mathbb{R}, \leq)$ be the usual linear order of real numbers and let $X \subseteq \mathbb{R}$ be such that the linear suborder $(X, \leq)$ is a well ordering. Show that then X is at most countable.*

The last theorem is taken from the book

Ch. S. Hardin and A. D. Taylor, *The Mathematics of Coordinated Inference*, Springer, 2013.

THANK YOU FOR YOUR ATTENTION!

HOMEWORK: Exercises 6, 7, 13 and 21. Deadline is the end of the coming Monday. Please, send me your solutions by e-mail to klazar@kam.mff.cuni.cz. To get credits for the tutorial, you should solve (or at least send in attempted solutions of) at least half of the homework exercises.