Kolgomorov-Veloso Problems and Dialectica Categories

Valeria de Paiva (Topos Institute) Samuel G. da Silva (UFBA)

July 2020

Dedicatory. This work is dedicated to Professor Paulo Veloso with our deepest appreciation for all he has done for research and teaching in Logic and Theoretical Computer Science in Brazil. Personally Professor Veloso has been a friend and mentor to both of us. He was also kind enough to accept to supervise me (Valeria de Paiva) knowing that I would be leaving the program, if my scholarship abroad was granted, which did happen. For this and many other acts of kindness, academic and personal, we are grateful and happy to celebrate his strong influence in our work.

1 Introduction

Blass' seminal paper [2] makes a surprising connection between Dialectica categories [16], Vojtáš' methods to prove inequalities between cardinal characteristics of the continuum [24] and the complexity theoretical notions of problems and reductions developed in [9]. Blass did not mention Kolmogorov's [10] very abstract notion of *problem*, which is not related to specific complexity issues. Kolmogorov did investigate a notion of abstract problem, producing an alternative intuitive semantics for Propositional Intuitionistic Logic, part of the celebrated BHK interpretation of Intuitionistic Logic.

Kolmogorov's problems were cited as an inspiration by Veloso when he developed his own theory of abstract problems in the Eighties [22], but the two frameworks were not formally connected. This note recalls Veloso's 'Teoria de Problemas' (Theory of Problems) and shows how it can be related to the Dialectica construction [15], via Kolmogorov's concepts. To establish this relationship, we use the modification of the Dialectica construction considered by the second author [20, 19] for other set-theoretical purposes. This modification corresponds to a condition of non-triviality of the collections of problems or solutions, first suggested by [13].

The categorical connection between Dialectica models, Kolmogorov's problems, Veloso's problems and Blass' problems shows that the use of categories really allows us to connect extremely different areas of mathematics, using simple methods. In the case of this paper, it also allow us to determine where exactly the foundational choices of axioms are important. We show that while Blass and Kolmogorov's notions of problem can be investigated using the set-theoretical framework of **ZF**, Veloso's problems commit us to a stronger set-theory, as discussed in the following sections. Whether this requirement of stronger foundations is a bug or a feature depends, perhaps, on personal taste and conviction. From our part we are happy to note that, like many other questions in Mathematics, as soon as one investigates them a little, the notion of 'problem' points out to grand challenges in the foundations of Mathematical Logic, to wit whether one wants to accept or not the Axiom of Choice within their chosen framework.

2 Kolmogorov Problems

Blass [2] noticed that de Paiva's Dialectica construction GC [15], when the base category C is the category **Sets**, is the dual of Vojtáš's category GT of generalized Galois-Tukey connections. Since the Dialectica construction has been generalized in many different directions, instead of writing $G\mathbf{Sets}$ we will write $\mathrm{Dial}_2(\mathbf{Sets})$ for this category, to make explicit the object 2 (the object of truth-values) where our relations map into, as well as the category C that is **Sets**, where objects 'live'. We recall the definition of the category below.

Definition 2.1 (Dialectica category [15])**.** *The category $Dial_2(\mathbf{Sets})$ has as objects triples of the form $A = (U, X, \alpha)$, where U and X are sets and $\alpha \subseteq U \times X$ is a set-theoretical relation, which can be written, equivalently, as $\alpha : U \times X \to 2$. If $A = (U, X, \alpha)$ and $B = (V, Y, \beta)$ are objects of $Dial_2(\mathbf{Sets})$, a morphism from A to B is a pair of functions in* **Sets**, *(f, F), $f : U \to V$, $F : Y \to X$ such that*

$$\textit{For all } u \in U \textit{ and } y \in Y,\ u\alpha F(y) \textit{ implies } f(u)\beta y.$$

Blass also noticed that the opposite, dual Dialectica Category $\mathrm{Dial}_2(\mathbf{Sets})^{\mathrm{op}}$ can be taken to intuitively mean that objects represent *problems* and morphisms stand for reductions between problems. Thus a triple $P = (I, S, \sigma)$ of $\mathrm{Dial}_2(\mathbf{Sets})^{\mathrm{op}}$, under this interpretation, represents a problem, whose instances are elements of I, the set of possible solutions is given by S and the relation σ can be read as "is solved by", that is, if z is an instance of the problem P and s is a possible solution then $z\sigma s$ states that "s solves z". Blass associates these problems with a concept of many-one reduction of search problems in complexity theory, a very restricted kind of problem, for which he refers to [9, 23].

Veloso's theory of problems ([22]), following Pólya, suggests that in order to understand a problem one should consider the following initial questions:

1. What is the unknown?
2. What are the data?
3. What is the condition?

These questions correspond directly to the elements of the triples of information which characterize a problem, which will be referred to, in this work, as a *Kolgomorov problem*. They also correspond precisely to Blass' interpretation above.

Definition 2.2 (Kolgomorov problems)**.** *A* **Kolgomorov problem** *is a triple $P = (I, S, \sigma)$, where I and S are sets and $\sigma \subseteq I \times S$ is a set theoretical relation. We say that:*

- *I is the set of* **instances** *of the problem P;*
- *S is the set of* **possible solutions** *for the instances I; and*
- *σ is the* **problem condition**, *i.e. the relation σ holds between z and s, in symbols $z\,\sigma\,s$ if the solution s satisfies the problem condition σ for the instance z, or, more briefly, "s σ-solves z".*

Kolmogorov's paper [10] has two parts. About the first section, which introduces his problems, he says that "If the intuitionistic cognitive presuppositions are not accepted then one should take into account only the first section". In this section he introduces problems via mathematical

examples, for instance "Find any four integers, x, y, z and n such that $x^n + y^n = z^n$, for $n > 2$". (Note that Kolmogorov states explicitly, in page 152, that "We never assume a problem to be solvable".)

We can identify the *objects* of the category $\mathrm{Dial}_2(\mathbf{Sets})$ with Kolgomorov problems. What would the *morphisms* represent in this case? To answer this, we consider the morphisms of the opposite of the Dialectica category, $\mathrm{Dial}_2(\mathbf{Sets})^{\mathrm{op}}$. In $\mathrm{Dial}_2(\mathbf{Sets})^{\mathrm{op}}$, a morphism from an object $P' = (I', S', \sigma')$ to an object $P = (I, S, \sigma)$ is a pair of functions (f, F), where $f\colon I \to I'$ and $F\colon S' \to S$ are such that the following condition holds

$$(\forall z \in I)\ (\forall t \in S')\ [f(z)\,\sigma'\,t \longrightarrow z\,\sigma\,F(t)].$$

So for all instances of problems z of P and all solutions of problems t of P', if the instance of problem $f(z)$ has σ'-solution t then the instance z has σ-solution $F(t)$.

If we regard P and P' as Kolgomorov problems, the existence of a morphism from P' to P ensures that there is a *reduction* of the problem P to the problem P' – because the act of solving an instance of P may be reduced to the act of solving an instance of P'. More precisely, if one wants to solve a particular instance z of the Kolgomorov problem P, it suffices to find a solution t for the instance $f(z)$ of P' – since $F(t)$ will provide a solution for the initial instance z of P.

Kolmogorov discusses a few number-theoretical and geometrical problems, as well as abstract, logical rules ones. In what follows, we present a number of examples from daily mathematical practice to show how they are coded as Kolgomorov problems. We also show reductions between those problems which can be seen as morphisms of $\mathrm{Dial}_2(\mathbf{Sets})^{\mathrm{op}}$. As a piece of notation, if X is a set and $n \in \mathbb{N}$ then $[X]^n$ denotes the family of all subsets of X which have precisely n elements and $[X]^{\leqslant n}$ means $\bigcup_{m \leqslant n} [X]^m$.

Example 2.3. *Analytical geometry is entirely based on the reduction of geometrical problems to equation solving problems.*

We present some practical examples to explain what we mean by the statement above.

Let π be any plane of the 3-dimensional Euclidean space $\mathbb{R}^3$ and let $F\colon \mathbb{R}^2 \to \pi$ be a coordinate system as usual (i.e., for every pair (u, v) of real numbers we associate the point $P = F(u, v)$ of the plane which has coordinates (u, v) – that is, $P = P_{(u,v)}$). Every line l of the plane π is then represented by an equation of the form $ax + by = c$, where a and b are real numbers such that $a \neq 0$ or $b \neq 0$ and $c \in \{0, 1\}$. Let E be the family of all equations of the described canonical form and let $\mathcal{L}$ denotes the family of all lines of the plane π. The decision problem of "whether a given point lies on a given line" is $(\mathcal{L}, \pi, \ni)$, and the problem of "whether a given pair of real numbers satisfy a given equation" is $(E, \mathbb{R}^2, \zeta)$, on which an equation $ax + by = c$ is ζ-related to a pair (u, v) of real numbers if $au + bv = c$. Then we can reduce the geometrical problem $(\mathcal{L}, \pi, \ni)$ to the algebraic problem $(E, \mathbb{R}^2, \zeta)$ using the morphism (f, F), where $f : \mathcal{L} \to E$ is defined by putting $f(l) = \mathrm{eq}(l)$ (where $\mathrm{eq}(l)$ is the canonical equation which represents l) and $F : \mathbb{R}^2 \to \pi$ is the coordinate system. Indeed, if (u, v) satisfies the equation of a line l we know that the corresponding point $P_{(u,v)}$ lies in l.

A slight variation of what we have just done reduces the problem of finding the intersection point of two distinct lines to the problem of solving a linear system with two equations over two variables. The geometrical problem of finding the intersection point of two distinct lines is $([\mathcal{L}]^2, \pi, \xi)$, where $\{l_1, l_2\}\,\xi\,P$ means that $P \in l_1 \cap l_2$ for any distinct lines l_1, l_2 of π and for every point P in π. The algebraic problem of finding the solution for a linear system with two equations over two variables is $([E]^2, \mathbb{R}^2, \lambda)$, where the relation λ in $\{a_1x + b_1y = c_1, a_2x + b_2y = c_2\}\lambda(u, v)$

is the conjunction of "$a_1x + b_1y = c_1$"$\zeta(u, v)$ and "$a_2x + b_2y = c_2$"$\zeta(u, v)$. The morphism which gives the reduction is (g, F), where $g : [\mathcal{L}]^2 \to [E]^2$ is given by $g(\{l_1, l_2\}) = \{f(l_1), f(l_2)\} = \{\text{eq}(l_1), \text{eq}(l_2)\}$ for all distinct lines l_1, l_2 of π and $F : \mathbb{R}^2 \to \pi$ is still the coordinate system. Now, if l_1 and l_2 are distinct lines and (u, v) is a solution of the system $\{\text{eq}(l_1), \text{eq}(l_2)\}$ then the point $P_{(u,v)}$ lies in the intersection of the lines l_1 and l_2.

Example 2.4. *The problem of finding vectors in the intersection of the kernels of a finite family of linear functionals over $\mathbb{R}^n$ reduces to the problem of finding the solutions of a homogeneous system of linear equations.*

Let $n \geqslant 2$ and $\{e_1, e_2, \ldots, e_n\}$ denote the canonical basis of the n-dimensional Euclidean space $\mathbb{R}^n$, regarded as a vector space over $\mathbb{R}$. A *linear functional* over $\mathbb{R}^n$ is a linear transformation from $\mathbb{R}^n$ into $\mathbb{R}$. Let $(\mathbb{R}^n)^*$ (the *dual* of $\mathbb{R}^n$) denote the family of all linear functionals over $\mathbb{R}^n$. It is well-known that the dimension of the dual space is also n, and that $\{\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_n}\}$ is a basis of the dual space – where, for $1 \leqslant i \leqslant n$, $\mathbf{x_i} : \mathbb{R}^n \to \mathbb{R}$ is the linear functional which satisfies $\mathbf{x_i}(e_j) = \delta_{ij}$ (where $\delta_{ij} = 1$ if $i = j$ and it is zero otherwise) for $1 \leqslant j \leqslant n$ and is then extended to all linear functionals by linearity.

Let $\mathcal{E}$ denote the family of all linear equations of the form $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0$, where $a_1, \ldots, a_n$ are real numbers. A linear functional $\mathbf{T}$ in the dual space of $\mathbb{R}^n$ may be written, in a unique way, in the form $T = \sum_{i=1}^{n} a_i\mathbf{x_i}$. Thus we may define a translation function $g : (\mathbb{R}^n)^* \to \mathcal{E}$ in the obvious way, i.e. by putting

$$g(T) = \text{“}a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0\text{”}$$

if $T = \sum_{i=1}^{n} a_i\mathbf{x_i}$.

The problem of finding vectors in the intersection of the kernel of finite families of linear functionals is $([(\mathbb{R}^n)^*]^{\leqslant n}, \mathbb{R}^n, \alpha)$, where $\mathcal{H}\,\alpha\,(c_1, c_2, \ldots, c_n)$ means that $(c_1, c_2, \ldots, c_n) \in \bigcap_{h\in\mathcal{H}} \text{Ker}(h)$ for any finite family $\mathcal{H}$ of m linear functionals with $m \leqslant n$ and any n-tuple $(c_1, c_2, \ldots, c_n) \in \mathbb{R}^n$ (recall that the dimension of the dual space is n as well, so we may only consider finite families with no more than n linear functionals). The problem of solving a homogeneous system of no more than n linear equations is $([\mathcal{E}]^{\leqslant n}, \beta, \mathbb{R}^n)$, where $\mathcal{G}\,\beta\,(c_1, c_2, \ldots, c_n)$ means that, for any $(c_1, c_2, \ldots, c_2) \in \mathbb{R}^n$ and any $\mathcal{G} \in [E]^m$ with $m \leqslant n$, $(c_1, c_2, \ldots, c_2)$ solves each one of the m linear equations of the finite family $\mathcal{G}$. A morphism which codes the usual and easily verifiable procedure of reducing the first problem to the second is now given by (f, Id), where $f : [(\mathbb{R}^n)^*]^{\leqslant n} \to [\mathcal{E}]^{\leqslant n}$ is given by $f(\mathcal{H}) = \{g(h) : h \in \mathcal{H}\}$ for any finite family $\mathcal{H}$ of no more than n linear functionals and Id is the identity function from the *set* $\mathbb{R}^n$ into the *vector space* $\mathbb{R}^n$ – i.e., we have reduced a problem stated in the context of the linear structure of $\mathbb{R}^n$ and its dual to a more naive, pedestrian problem of finding solutions of a homogeneous system of equations.

Veloso developed further notions of *viable problems*, *links* between problems (and *reduction links* between problems) in his theory of mathematical problems [22]. However, as Veloso himself was aware of (see further discussion in the final section), these definitions make essential use of the Axiom of Choice ([11],[12]), and this use will be detailedly discussed in the next section.

3 Veloso Problems and the Axiom of Choice

In our previous work [20] we described a modification of the category $\mathrm{Dial}_2(\mathbf{Sets})^{\mathrm{op}}$, which Blass calls the category $\mathcal{PV}$ in [2]. Blass, describing the category $\mathcal{PV}$, explains that it has as objects problems, together with their instances and respective solutions. Moreover, morphisms of the category $\mathcal{PV}$ identify reductions of classes of (complexity) problems to others. The modification of the category in [20], following the work of [13], insists on some conditions of non-triviality of the objects. These conditions can be paraphrased as 'there are no problems without a solution' and 'there are no solutions that solve all problems at once'. There are also some constraints on the cardinality of the sets of instances and solutions of $\mathcal{PV}$; all constituent sets of objects of $\mathcal{PV}$ are bounded above by the cardinality of the *continuum* (which is $\mathfrak{c} = 2^{\aleph_0} = |\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$).

The mentioned non-triviality conditions are not found in the original Dialectica categorical construction ([15],[16]), where trivial objects are actually required to provide truth-values (or units for the categorical operators) associated to the logical connectives of Girard's Linear Logic [6]. The non-triviality conditions are also not found in Kolmogorov's work. He describes *meaningless* problems as the ones that do not have a solution.

The non-triviality conditions will characterize, exactly, a class of problems we refer to as *Veloso problems*. We note, however, that there are no upper bounds for the cardinality of the sets of instances and solutions of the problems originally discussed by Veloso.

We first formally present the category $\mathcal{PV}$, as well as stratified versions of it which were introduced in [19]. The following definition should be considered within **ZFC**, since we refer to well-ordered cardinals in its first clause.

Definition 3.1 (Category $\mathcal{PV}$ [20])**.** *The category $\mathcal{PV}$ is the subcategory of $Dial_2(\mathbf{Sets})^{op}$ whose objects are the triples $A = (U, X, \alpha)$ satisfying the following three clauses, which will be referred to as the* **MHD** *conditions (***MHD** *stands for Moore, Hrušák and Džamonja [13]):*

(1) The cardinalities of the (non-empty) constituent sets are bounded above by the cardinality of the continuum – i.e. $0 < |U|, |X| \leqslant 2^{\aleph_0}$.

(2) Every problem has a solution – i.e.

$$(\forall u \in U)(\exists x \in X)[u \,\alpha\, x].$$

(3) There are no solutions that solve all the problems at once – i.e.

$$(\forall x \in X)(\exists u \in U)[\neg\, (u \,\alpha\, x)].$$

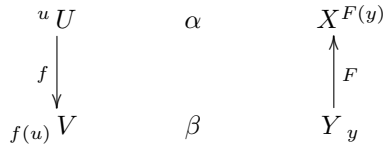
The morphisms between objects of $\mathcal{PV}$ are the same morphisms of $Dial_2(\mathbf{Sets})^{op}$ – that is, a morphism from an object $B = (V, Y, \beta)$ to an object $A = (U, X, \alpha)$ is a pair of functions (f, F), where $f : U \to V$ and $F : Y \to X$ are such that

$$(\forall u \in U)\ (\forall y \in Y)\ [f(u)\, \beta\, y \longrightarrow u \,\alpha\, F(y)].$$

Morphisms of $\mathcal{PV}$ induce the **Galois-Tukey pre-order** introduced by Vojtáš, which is defined in the following way: if $A = (U, X, \alpha)$ and $B = (V, Y, \beta)$ are objects of $\mathcal{PV}$, then we have

$$A \leqslant_{GT} B \iff \text{There is a morphism from } B \text{ to } A.$$

The diagram below represents the situation where $A \leqslant_{GT} B$:



Given an object $A = (U, X, \alpha)$ of $\mathcal{PV}$, its *dual object* is given by $A^* = (X, U, \alpha^*)$, where $x\alpha^* u$ means that $\neg\,(u\alpha x)$. One can easily check (via a contrapositive argument) that:

$$\text{If } A \leqslant_{GT} B, \text{ then } B^* \leqslant_{GT} A^*.$$

In [19] parametrized, stratified versions of $\mathcal{PV}$ were introduced – the $\mathcal{PV}_X$ categories, for X an infinite set. The main goal of the proposed stratification was to generalize features of $\mathcal{PV}$ to sets of higher cardinalities, since the constituents of the objects of $\mathcal{PV}$ are bounded above by the cardinality of the continuum (which is the cardinality of the power set of the naturals). Notice that, indeed, in **ZFC** the categories $\mathcal{PV}$ and $\mathcal{PV}_{\mathbb{N}}$ coincide, and so the whole idea of the stratified versions was to generalize $\mathcal{PV}$ (in a choiceless context) to any other other infinite set X. These categories are introduced in the **ZF** setting, as their definitions use the notion of *domination* ($\preccurlyeq$) between sets instead of that of well-ordered cardinals (for a more detailed discussion on the subtleties of comparing sizes in the absence of **AC**, we refer to Section 2 of [19]). Recall that a set A is *dominated* by a set B, $A \preccurlyeq B$, if there is an injective function from A into B.

Definition 3.2 (Categories $\mathcal{PV}_X$)**.** *Let X be an infinite set in* **ZF**. *Then $\mathcal{PV}_X$ is the subcategory of $Dial_2(\mathbf{Sets})^{op}$ whose objects (U, X, α) are those which satisfy the following $\mathbf{MHD}_X$ conditions (since they are a restricted form of the* **MHD** *conditions):*

(1) U, V are non-empty sets and $U, V \preccurlyeq \mathcal{P}(X)$, that is, sets U, V are dominated by $\mathcal{P}(X)$.

(2) $(\forall u \in U)(\exists x \in X)[u\,\alpha\,x]$

(3) $(\forall x \in X)(\exists u \in U)[\neg\,(u\,\alpha\,x)]$

The morphisms between objects of $\mathcal{PV}_X$ are the same morphisms of $Dial_2(\mathbf{Sets})^{op}$.

We also define, in the expected way, a Galois-Tukey ordering $\leqslant_{GT}$ on the objects of $\mathcal{PV}_X$.

The categories $\mathcal{PV}_X$ are used in [19] to provide, after a quantification over all infinite sets, equivalences of the Axiom of Choice **AC**. The following equivalences are proved in [19]:

Theorem 3.3 (da Silva [19])**.** *The Axiom of Choice is equivalent to the following statements:*

(*) "For every infinite set X, $(\mathcal{P}(X), \mathcal{P}(X), =)$ is a maximum element in the Galois-Tukey ordering $\leqslant_{GT}$ on $\mathcal{PV}_X$."

and

(**) "For every infinite set X, $(\mathcal{P}(X), \mathcal{P}(X), \neq)$ is a minimum element in the Galois-Tukey ordering $\leqslant_{GT}$ on $\mathcal{PV}_X$."

This theorem shows that stratifying objects and features of the Dialectica construction using the Galois-Tukey ordering is equivalent to accepting the Axiom of Choice. This may be a surprise to mathematicians not used to the "thinking about foundational issues" exercise.

In this work we are interested in the investigation of general problems, which means that, in particular, the sets of instances and solutions should have no upper bounds on their cardinalities. To do so in a categorical setting, we provide the following definition, which should be considered in the setting of **ZF**.

Definition 3.4 (Unbounded $\mathcal{PV}$ category)**.** *The category $\mathcal{PV}_{unb}$, the unbounded $\mathcal{PV}$ category, is the the subcategory of $Dial_2(\mathbf{Sets})^{op}$ whose objects (U, X, α) satisfy the* **MHD** *conditions (2) and (3) but where the* **MHD** *condition (1) is relaxed to allow sets of arbitrary large cardinality. Thus we require* **MHD** *conditions (2) and (3) together with*

(1)' U and X are non-empty sets

A triple (U, X, α) is an object of $\mathcal{PV}_{unb}$ if it is an object of $\mathcal{PV}_Y$ for some infinite set Y.

The morphisms between objects of $\mathcal{PV}_{unb}$ are the very same morphisms of $Dial_2(\mathbf{Sets})^{op}$.

The unbounded $\mathcal{PV}$ category captures, precisely *Veloso problems* – these are the Kolgomorov problems which are **viable** and **non-generic**, as we define now.

Definition 3.5 (Veloso problem)**.** *Let $P = (I, S, \sigma)$ be a Kolgomorov problem.*

(i) P is said to be a **viable** *problem if the domain of σ is the whole set I – or, equivalently, if for every instance z of I there is some possible solution s in S that solves the problem, so that the relation $z\,\sigma\,s$ holds.*

(ii) A possible solution s will be said to be a **generic solution** *for P if it solves all of its instances – that is, if for every instance z of I one has $z\,\sigma\,s$ for this particular solution s.*

(iii) The problem P is said to be **non-generic** *if it has no generic solutions – equivalently, for every possible solution $s \in S$ there is some instance $z \in I$ such that $\neg(z\sigma s)$.*

(iv) P will be said to be a **Veloso problem** *if it is viable and non-generic.*

Notice that the fact that a problem $P = (I, S, \sigma)$ is non-generic is equivalent to the viability of the dual problem $P^* = (S, I, \sigma^*)$, where $s\,\sigma^*\,z$ means $\neg(z\sigma s)$ for all $z \in I$ and $s \in S$.

It should be clear that viability and non-genericity are conditions asking for non-triviality of a given problem. For instance, it is well-known that the following statement is an Axiom of Incidence, in Hilbert's plane geometry:

(†) *"For every line l, there are at least two points which lie in the line l and at least one point which does not lie in the line l"*

Together with the axiom "For every pair of distinct points there is only one line which passes through those points", the above statement (†) corresponds, precisely, to the viability and non-genericity requirements for the problem of determining whether a given line contains a given pair

of distinct points of the plane or $(L, P, \supseteq)$, where

L = the set of all lines of the plane; and

P = the family of all pairs of two distinct points of the plane.

Notice also that non-genericity establishes a dimension for the preceding problem: if all points were in the same line l we would not be studying the geometry of the plane, only the geometry of a line.

The following example shows that certain mathematical notions are equivalent to the viability of certain problems. Recall that a subset of a topological space is *dense* if its closure is equal to the whole space. It is a textbook easy exercise to show that dense sets are precisely those which intersect any non-empty open set. Thus, the following holds:

Example 3.6. *Let (X, τ) be topological space and D be a proper subset of X. Then D is a dense subspace of X if, and only if, the Kolgomorov problem $(\tau \setminus \{\emptyset\}, D, \ni)$ is viable.*

Alternatively, D is a dense set if, and only if, for every non-empty open set U of X the problem $(\{U\}, D, \ni)$ is viable. This observation is relevant in the following example, which is, accordingly to Veloso ([22], page 24), a *problem to prove* in Pólya's terminology – in contrast to the so-called *problems to find*. Recall that a topological space is a *Baire space* if the intersection of any countable family of dense subsets of the space is also dense subset of the space.

Example 3.7. *To prove the Baire Theorem for Complete Metric Spaces (i.e., the theorem which asserts that any complete metric space is a Baire space), it suffices to verify that, for any non-empty open set O and for any countable family $\{U_n : n \in \mathbb{N}\}$ of dense open sets, the problem $(\{O\}, \bigcap_{n\in\mathbb{N}} U_n, \ni)$ is a viable problem.*

Later on we will show that the above example is easier to handle if transformed into a countable chain of viable related problems.

The notion of *viability* of a problem, introduced by Veloso in [22] (page 25), is related to the notion of *solvability* of the problem. However, a solution of a problem for Veloso is represented by a function, not by a relation, as it is the case in our work. We will use the terminology *solution function* to denote these objects that are, instead of solution relations, solution functions.

Definition 3.8. *Let $P = (I, S, \sigma)$ be any viable Kolgomorov problem. A* **solution function** *for P is a function $f : I \to S$ satisfying $f \subseteq \sigma$ – or, equivalently, f is a S-valued function with domain I such that for every instance z of P we have that $f(z)$ solves z.*

Veloso (op. cit) has defined a notion of solvability according to his definition of solution – that is, in our terms, a Kolgomorov problem P is **solvable** if P has a solution function. As one of the easiest equivalent statements of the Axiom of Choice is precisely *"Every relation contains a function with the same domain"* (see page 131 of [12]), it is straightforward to check that, within **ZFC** (i.e., assuming the Axiom of Choice), the following equivalences hold:

Proposition 3.9 (viable is solvable in **ZFC**)**.** *Let $P = (I, S, \sigma)$ be any Kolgomorov problem. The following statements are equivalent:*

(i) The Kolmogorov problem P is viable.

(*ii*) *The problem P is solvable.*
(*iii*) *The problem P satisfies the formula $(\forall z \in I)(\exists s \in S)[z\,\sigma\,s]$.*

The preceding proposition was also stated by Veloso. The only non-obvious implication ($(i) \longrightarrow (ii)$) follows easily from the equivalence of the Axiom of Choice mentioned above.

Still following Veloso's definitions from [22], next we define the notions of *links* and *reduction links* between problems. We point out that the notion of "reduction link" will be defined in terms of "solution functions". Again, this context is intrinsically associated to the Axiom of Choice, as we will discuss later.

Definition 3.10 (Links and reduction links [22])**.** *Let $P = (I, X, \sigma)$ and $P' = (I', X', \sigma')$ be two Kolgomorov problems.*

(*i*) *A* **link** *from P to P' is a pair of functions (f, F), where*

$f : I \to I'$ is said to be a **translation function***; and*
$F : S' \to S$ is said to be a **recovery function**.

(*ii*) *A link (f, F) from P to P' is called a* **reduction link** *of P to P' if it lifts solution functions from P' to P, i.e. for every solution function g of P' the composite function $F \circ g \circ f$ is a solution function for P.*

From now on we identify the class of all Veloso problems with the objects of the category $\mathcal{PV}_{\text{unb}}$. Next we show that morphisms of this category correspond to reduction links between the corresponding problems.

Proposition 3.11. *Let $P = (I, X, \sigma)$ and $P' = (I', X', \sigma')$ be objects of $\mathcal{PV}_{unb}$, considered as Kolgomorov problems. If (f, F) is a morphism witnessing the order $P \leqslant_{GT} P'$, then (f, F) is a reduction link of P to P'.*

Proof:. Let g be an arbitrary solution function for the problem P'. As we know that (f, F) is a morphism from P' to P, we know that for all $z \in I$ and $t \in S'$ the following implication holds:

$$f(z)\,\sigma'\,t \longrightarrow z\,\sigma\,F(t)$$

Fix an arbitrary $z \in I$. As $g \subseteq \sigma'$, for $t = g(f(z))$ we have that $f(z)\,\sigma'\,t$, and therefore

$$z\sigma F(t) = F(g(f(z))$$

and thus $(z, F(g(f(z)) \in \sigma$. By the arbitrariness of z, we conclude that $F \circ g \circ f \subseteq \sigma$ and so the composite function $F \circ g \circ f$ is a solution function for P, as desired. ■

So, given Kolgomorov problems P and P' with a Dialectica morphism (f, F) witnessing the inequality $P \leqslant_{GT} P'$ in the Galois-Tukey ordering, we are allowed to interpret such inequality as a measure of complexity, since a solution of P may be reduced to a solution of P' – thus under $P \leqslant_{GT} P'$ we can say that P is as easy to solve as P', or that P is not more complicated to be solved than P'.

We have shown that the existence of solution functions for viable problems is ensured by the Axiom of Choice (Proposition 3.9). As Veloso's reduction links were defined in terms of solution functions, it is clear that this approach presupposes a choice principle. In the following results, we will show more, as it will be established that assuming that Veloso's approach holds

in full generality gives rise to a number of equivalents of the Axiom of Choice (or of weak related statements). For the rest of this section, our base theory is **ZF**.

Theorem 3.12. **AC** *is equivalent to the following statement:*

"Every Veloso problem has a solution function".

Proof:. ($\Rightarrow$) Let $P = (I, S, \sigma)$ be a Veloso problem. By the **MHD** condition (1), P is viable and so $dom(\sigma) = I$. As in the proof of Proposition 3.9, the existence of a solution function is guaranteed by the equivalent of **AC** given by the statement "Every relation contains a function with same domain".
($\Leftarrow$) It was remarked in [19] that **AC** is equivalent to the following statement:

"For every infinite set X, there is a choice function defined on $\mathcal{P}(X) \setminus \{\emptyset\}$ – that is, there is $f : \mathcal{P}(X) \setminus \{\emptyset\} \to X$ such that $f(Y) \in Y$ for all $\emptyset \neq Y \subseteq X$."

So, let X be any infinite set. The problem

$$(\mathcal{P}(X) \setminus \{\emptyset\}, X, \ni)$$

is clearly viable (since non-empty subsets have elements, by definition) and non-generic (given $x \in X$ one has that $Y = X \setminus \{x\}$ is not solved by x). A solution function for this problem is, clearly, a choice function for $\mathcal{P}(X) \setminus \{\emptyset\}$. As X was taken arbitrarily, we have established **AC** by the above remark. ■

It follows from the previous theorem that in the absence of the Axiom of Choice there will be Veloso problems in $\mathcal{PV}_{\text{unb}}$ without any solution function.

Notice that, if P' is a Veloso problem without a solution function, it is vacuously true that *any link* from P to P' (for *any* given P) is a reduction link. Motivated by this, we introduce the following definition:

Definition 3.13. *Let P, P' be problems in $\mathcal{PV}_{unb}$. A morphism (f, F) from P' to P is said to be* **realized as a reduction link** *if the statement "(f, F) is a reduction link from P to P' " holds non-vacuously.*

If all morphisms have to be realized as reduction links, then the Axiom of Choice must be present, as the following theorem shows.

Theorem 3.14. **AC** *is equivalent to the statement*

"Every morphism of $\mathcal{PV}_{unb}$ is realized as a reduction link".

Proof:. ($\Rightarrow$) Given a morphism from P' to P, **AC** implies that P' has solution functions (by 3.12), and the rest follows from Proposition 3.11 and from the definition of "realized as a reduction link".
($\Leftarrow$) Given any infinite set X, we are able to consider the object of $\mathcal{PV}_{\text{unb}}$ given by

$$P = (\mathcal{P}(X) \setminus \{\emptyset\}, X, \ni).$$

and the corresponding identity morphism (id, id) from P to P. If we assume that (id, id) is realized as a reduction link then there is a solution link for P, which will be a choice function for

$$\mathcal{P}(X) \setminus \{\emptyset\}.$$

As X was taken arbitrarily, we obtain **AC** in the same way as in Theorem 3.12 ■

There are several set-theoretical statements which are referred to, in the literature, as *weak choice principles*. Weak choice principles are implied by the Axiom of Choice **AC**, but they are not equivalent to it, and are often regarded as "fragments" or "partial cases" of **AC**. To identify the precise amount of choice which is needed for a particular argument/result is a fruitful and current line of research (akin to Reverse Mathematics) within Set Theory. This may be seen in the standard reference [8] and in the dozens of papers which have cited it over the last twenty years.

The Axiom of Countable Choice (usually denoted by $\mathbf{AC}_\omega$) is one of the most celebrated weak choice principles. It corresponds to the restriction of the Axiom of Choice to countable families of non-empty sets, that is, it asserts that "Every countable family of non-empty sets has a choice function", or if $\{X_n : n \in \mathbb{N}\}$ if a countable family of non-empty sets then there is a function

$$f : \{X_n : n \in \mathbb{N}\} \to \bigcup_{n\in\mathbb{N}} X_n$$

such that $f(X_n) \in X_n$ for all $n \in \mathbb{N}$.

In the following theorem, we prove an equivalent of countable choice $\mathbf{AC}_\omega$ in terms of Veloso problems – more specifically, in terms of Veloso problems whose instance sets are countable.

Theorem 3.15. *The Axiom of Countable Choice* $\mathbf{AC}_\omega$ *is equivalent to the following statement:*

"Every Veloso problem whose set of instances is countable has a solution function".

Proof:. ($\Rightarrow$) Let $P = (I, S, \sigma)$ be a Veloso problem, on which the instance set I is a countable set. Enumerate $I = \{z_n : n \in \mathbb{N}\}$. As P is viable, we know that

$$(\forall n \in \mathbb{N})(\exists s \in S)[z_n \ \sigma \ s]$$

and so for every $n \in \mathbb{N}$ the set

$$F_n = \{s \in S : z_n \, \sigma \, s\}$$

is a non-empty set. Applying $\mathbf{AC}_\omega$ to the countable family of non-empty sets given by

$$\mathcal{F} = \{F_n : n \in \mathbb{N}\},$$

we get a choice function $g : \mathcal{F} \to \bigcup \mathcal{F}$ with $g \subseteq \sigma$ – so that $z_n \ \sigma \ g(F_n)$ for all $n \in \mathbb{N}$. A solution function f for the problem $P = (I, S, \sigma)$ is now easily defined by putting, for every $z \in I$,

$$f(z) = g(F_m) \iff z = z_m.$$

($\Leftarrow$) Let $\mathcal{F} = \{X_n : n \in \mathbb{N}\}$ be a countable family of non-empty sets. We have to show that there is a choice function for such family, i.e. we have to exhibit a function $f : \mathcal{F} \to \bigcup \mathcal{F}$ such that $f(X_n) \in X_n$ for all $n \in \mathbb{N}$.

Consider the set X given by

$$X = \bigcup_{n\in\mathbb{N}} (\{n\} \times X_n)$$

and let $\sigma \subseteq \mathbb{N} \times X$ be the binary relation defined in the following way:

$$n \, \sigma \, x \iff \Pi_1(x) = n,$$

where Π_1 denotes the projection on the first coordinate. In other words, for all $(m, z) \in X$ we have that $n\,\sigma\,(m, z)$ if, and only if, $n = m$.

Consider the problem $(\mathbb{N}, X, \sigma)$. As $\mathcal{F}$ is supposed to be a family of non-empty sets, such problem is viable, and (as $\mathbb{N}$ is infinite) it is easy to check that it is also non-generic. So, $(\mathbb{N}, X, \sigma)$ is a Veloso problem. By hypothesis, there is a solution function of $(\mathbb{N}, X, \sigma)$, say $g : \mathbb{N} \to X$. Now we define

$$f : \mathcal{F} \to \bigcup_{n\in\mathbb{N}} X_n$$

by putting

$$f(F_n) = \Pi_2(g(n))$$

for all $n \in \mathbb{N}$. It should be clear that f is a choice function for $\mathcal{F}$. ■

The reader may check that we could have proved versions of the three preceding theorems stated only in terms of viable problems. In fact, Veloso himself has observed that the equivalence between **AC** and the statement "Every viable problem has a solution" holds ([22], page 35). However, as the problem $(\mathcal{P}(X) \setminus \{\emptyset\}, X, \ni)$ is a Veloso problem (i.e., viable and non-generic) for any infinite set X – and it is, basically, the problem which appears in several parts of the proofs -, we have preferred to point out that the class of Veloso problems is enough, in each case, to provide an equivalence with the corresponding choice principle.

The final result of this section will be stated in terms of viable problems only. First, we will introduce the notion of $\aleph_0$*-chain of viable problems.*

Definition 3.16 (chain of viable problems)**.** *Let $\{I_n : n \in \mathbb{N}\}$ be a family of non-empty sets and $\{\sigma_n : n \in \mathbb{N}\}$ be a family of binary relations such that, for all $n \in \mathbb{N}$,*

$$\sigma_n \subseteq I_n \times I_{n+1}.$$

Let $S_n = I_{n+1}$ and $P_n = (I_n, S_n, \sigma_n)$ for all $n \in \mathbb{N}$. We say that $\langle P_n : n \in \mathbb{N}\rangle$ is an **$\aleph_0$-chain of viable problems** *if all problems P_n are viable, i.e. for all $n \in \mathbb{N}$ one has*

$$\forall z \in I_n\ \exists s \in S_n\ [z\,\sigma_n\,s].$$

The preceding definition aims to capture the very common situation in Mathematics on which one has to solve a $\mathbb{N}$-sequence of chained problems, where the solution of the n-th problem is an instance of the $(n + 1)$-problem. In such situation one wishes, of course, to produce a sequence of solutions.

Definition 3.17. *Let $\langle P_n : n \in \mathbb{N}\rangle$ be an $\aleph_0$-chain of viable problems, where $P_n = (I_n, S_n, \sigma_n)$ and $S_n = I_{n+1}$ for all $n \in \mathbb{N}$. A* **solution sequence** *for $\langle P_n : n \in \mathbb{N}\rangle$ is a sequence $\langle z_n : n \in \mathbb{N}\rangle$ such that $z_n \in I_n$ and $z_n\sigma_n z_{n+1}$ for all $n \in \mathbb{N}$.*

We present below a mathematical example where the above concepts play an important role.

Example 3.18. *The usual proof of the Baire Category Theorem for complete metric spaces given in the textbooks may be encoded by a $\aleph_0$-chain of viable problems.*

Let us see why. Let $\{U_n : n \in \mathbb{N}\}$ be a countable family of dense open sets of a complete metric space M and let O be an arbitrary non-empty open set (as in Example 3.7). We have to show that the intersection of all the U_n's meets O. We let I_n be the family of all non-empty open

sets whose diameter is less than $\frac{1}{n+1}$ and whose closures are included in $U_n \cap O$, and let σ_n be the reverse inclusion. It is easy to check that all of the problems $\langle I_n, S_n, \sigma_n \rangle$ (where $S_n = I_{n+1}$) are viable problems. If $\langle V_n : n \in \mathbb{N} \rangle$ is a solution sequence for such $\aleph_0$-chain of problems, then $\big(\bigcap_{n \in \mathbb{N}} U_n \big) \cap 0$ is ensured to be non-empty, since $\{\overline{V_n} : n \in \mathbb{N}\}$ is a decreasing sequence of non-empty closed sets whose diameters converge to zero, so it has non-empty intersection in the complete metric space M – and, by the definition of the I_n's, any point of such intersection testifies that $\big(\bigcap_{n \in \mathbb{N}} U_n \big) \cap 0 \neq \emptyset$.

What is usually not said in the textbooks about the preceding example is that a solution sequence for the $\aleph_0$-chain of viable problems is given by the *Principle of Dependent Choices*, denoted by **DC**, which is another celebrated weak choice principle[1]. The Principle of Dependent Choices states:

"If δ is a binary relation on a non-empty set A (i.e. $\delta \subseteq A \times A$) satisfying

$$(\forall x \in A)(\exists y \in A)[x \, \delta \, y],$$

then there is a sequence $\langle x_n : n \in \mathbb{N} \rangle$ of elements of A such that $x_n \, \delta \, x_{n+1}$ for all $n \in \mathbb{N}$".

The principle **DC** is regarded as the precise amount of choice needed to make a countable number of consecutive arbitrary choices. It is well-known that the Axiom of Choice is stronger than the Principle of Dependent Choice which is stronger than the Axiom of Countable Choice, i.e.

$$\mathbf{AC} \Rightarrow \mathbf{DC} \Rightarrow \mathbf{AC}_\omega,$$

and that none of those implications is reversible. More information on these and many other weak choice principles may be found in [8].

In what follows, we present equivalents of **DC** in terms of $\aleph_0$-chains of viable problems.

Theorem 3.19. *The following statements are equivalent:*

(i) The Principle of Dependent Choices, **DC***;*

(ii) For any $\aleph_0$-chain of viable problems $\langle P_n : n \in \mathbb{N} \rangle$ (where, for all $n \in \mathbb{N}$, $P_n = (I_n, S_n, \sigma_n)$ and $S_n = I_{n+1}$) and for every instance $z \in I_0$, there is a solution sequence $\langle z_n : n \in \mathbb{N} \rangle$ for this $\aleph_0$-chain with $z_0 = z$; and

(iii) Every $\aleph_0$-chain of viable problems has a solution sequence.

Proof:.$(i) \Rightarrow (ii)$: Let $\langle P_n : n \in \mathbb{N} \rangle$ be as in the statement. We define a set A whose elements are, precisely, all $(k+1)$-tuples

$$(z_0, z_1, \ldots, z_k),$$

where k ranges over all natural numbers, $z_0 = z$, $z_i \in I_i$ for all $0 \leqslant i \leqslant k$ and also $z_i \, \sigma_i \, z_{i+1}$ for all $0 \leqslant i \leqslant k-1$ if $k > 0$. We define, over the tuples of A, a relation δ such that

$$(w_0, w_1, \ldots, w_k) \, \delta \, (t_0, t_1, \ldots, t_j)$$

if $k < j$ and $w_i = t_i$ for all $0 \leqslant i \leqslant k$ – that is, δ is the usual strict prefix order over the tuples.

As all of the problems of the $\aleph_0$-chain are viable by definition, it is easy to check that the set A and the relation δ satisfy the requirements one needs to apply the Principle of Dependent Choices. So, by **DC**, there is a sequence $\langle s_n : n \in \mathbb{N} \rangle$ of tuples such that $s_n \, \delta \, s_{n+1}$ for all $n \in \mathbb{N}$.

[1] In fact, the Principle of Dependent Choices is *equivalent* to the Baire Theorem for complete metric spaces, as shown in [1].

If we identify each tuple with the corresponding finite sequence, we get a compatible family of functions (in fact, an increasing chain of compatible finite functions), and so the union of such family is a function. It is easy to check that the obtained sequence $z = \bigcup_{n\in\mathbb{N}} s_n$ is a solution sequence for the $\aleph_0$-chain with $z_0 = z$, as desired.

$(ii) \Rightarrow (iii)$: Obvious.

$(iii) \Rightarrow (i)$: If A and δ are under the hypothesis of **DC**, then A is a non-empty set and (A, A, δ) is a viable problem. Then we just have to consider the $\aleph_0$-chain $\langle P_n : n \in \mathbb{N}\rangle$ where $I_n = S_n = A$ and $\sigma_n = \delta$ for all $n \in \mathbb{N}$. By (iii) we may assume that there is a solution sequence for this $\aleph_0$-chain, say $\langle z_n : n \in \mathbb{N}\rangle$. So, this sequence satisfies $z_n \,\delta\, z_{n+1}$ for all $n \in \mathbb{N}$. As A and δ were taken arbitrarily, we have just established **DC** – and the proof is then finished. ■

We have shown that the Axiom of Countable Choice, the Principle of Dependent Choices and the fully-fledged Axiom of Choice correspond to natural (sub-)classes of problems, as described by Kolmogorov and Veloso.

4 Tight Coupled Problems

In this short section we discuss how the notion of a "tight coupled reduction link" between problems can be seen as a previously known variant of the Dialectica construction we have discussed so far.

The way in which the notion of *reduction link* of P to P' was defined (item (ii) of Definition 3.10) seems to suggest that there is no tight connection or "coupling", in general, between problems P and P' – as pointed out by Veloso in the page 28 of [22]. Veloso argues that a reduction link of P to P' is, in most cases, *uncoupled* in the following sense: after applying the translation function f on an instance z of P, we may forget completely about P and only care about solving the instance $f(z)$ of P' – and, after that, any solution $t \in S'$ of the instance $f(z)$ of P' will generate a solution of the instance z of P by applying the recovery function F. However, in certain situations (see example below), it is interesting to allow the use of some additional information during the recovery process.

For this case, Veloso defines *tightly coupled links* from P to P' in the following way: the translation function is still some $f : I \to I'$ but the recovery function is a function $F\colon I \times S' \to S$ so that the information on the original instance z of P may be used at the time of recovery – that is, the pair (f, F) needs to satisfy the following condition: for any $z \in I$ and any $t \in S'$,

$$f(z)\,\sigma'\,t \longrightarrow z\,\sigma\,F(z,t).$$

This requirement on the tightly coupled links corresponds, precisely, to the morphisms of the dual of Dial(**Sets**) (the simplest case of the "original" Dialectica category, inspired by Gödel's Dialectica Interpretation and introduced by the first author in [4]).

Example 4.1 (Reduction with tight coupled link)**.** *Using tight coupled links, one can formally prove that the problem of finding a normal line of a surface through a certain point is not more complicated than the problem of finding orthogonal planes to a certain plane.*

In this example, we use *surface* for a two-dimensional differential manifold $S \subseteq \mathbb{R}^3$, and therefore given a point $x \in S$ there is a tangent plane $T_x(S)$ centred at x. Recall that if x is a point of a plane $\pi \subseteq \mathbb{R}^3$ then a line l through x is the *normal line* of the plane π (through x) if l is perpendicular to all lines of π which go through x, and if x is a point of a surface S then

the normal line of S through x is the normal line of the tangent plane $T_x(S)$ through x. Two intersecting planes π and ρ are said to be *orthogonal* if for every point of the intersection line the normal lines of π are contained in ρ and vice-versa. Notice that if l is the normal line of a plane π through x then l is included in every plane ρ which is orthogonal to π and passes through x – in other words, all planes which are orthogonal to a given plane π and passes through a given point share the normal line of π through this very same point.

Let $\mathcal{L}$ be the family of all lines of the 3-dimensional Euclidean space $\mathbb{R}^3$ and $\mathcal{P}$ the family of all planes of $\mathbb{R}^3$. For a given surface S, the problem of finding the normal lines through each point of the surface is $(S, \mathcal{L}, \sigma)$, where $x\,\sigma\,l$ means "l is the normal line of S through x" for every point $x \in S$ and every line $l \in \mathcal{L}$, and the problem of finding orthogonal planes is $(\mathcal{P}, \mathcal{P}, \xi)$, where $\pi\,\xi\,\rho$ means "π and ρ are orthogonal planes" for all planes π and ρ in $\mathbb{R}^3$.

A tight coupled link from $(S, \mathcal{L}, \sigma)$ to $(\mathcal{P}, \mathcal{P}, \xi)$ is given by the pair (f, F), where $f : S \to \mathcal{P}$ is defined by putting $f(x) = T_x(S)$ for all $x \in S$ and $F\colon S \times \mathcal{P} \to \mathcal{L}$ is given by $F(x, \rho) = \varphi(T_x(S), \rho, x)$, where $\varphi : \mathcal{P} \times \mathcal{P} \times \mathbb{R}^3 \to \mathcal{L}$ is defined by putting $\varphi(\pi, \rho, x) =$ the line l contained in the plane $t(x, \rho)$ (where $t(x, \rho)$ is ρ itself if $x \in \rho$ or is the unique plane parallel to ρ passing through x otherwise) which is perpendicular to the intersecting line of π and $t(x, \rho)$ through x, if π and ρ are orthogonal planes; and any previously fixed line otherwise. In view of the fact remarked at the end of the previous paragraph, it is easy to see that $F(x, \rho)$ is the normal line of $T_x(S)$ through x (and thus, of S) whenever ρ is a plane orthogonal to $f(x) = T_x(S)$. Notice that the described reduction link formalizes the following mental procedure: "if I know how to produce an orthogonal plane for any given plane, then I know how to produce the normal line of a surface S at a point x: we take any plane ρ that is orthogonal to $T_x(S)$, translate it to x – via parallel translation – and then consider the perpendicular line (through x and contained in the translated plane) of the intersection line of $T_x(S)$ and the translated plane".

This shows one case where the information on the original problem instance (the original point x) is required for the recovery function F of the tight coupled link (f, F) that reduces the original problem of "finding normal lines to a given point in the surface" to the new problem of "finding orthogonal planes". This problem is particularly nice, as it seems to connect to approaches to automatic differentiation under development using categorical machinery in [5]. More research work is required here.

5 Conclusions and Further Work

We have shown that the work of Kolmogorov can be regarded as a bridge between the abstract problems Veloso discussed in his Theory of Mathematical Problems and the complexity problems Blass discussed in [2]. This bridge can be seen by means of the categorical Dialectica constructions GC and DC introduced in [16].

Veloso's *Critical Retrospect* in [22] already observed that his approach on viable Kolgomorov problems relies heavily on the Axiom of Choice and asks whether such approach (together with some suggested techniques on decomposition of problems) was "tainted" by **AC** – since the mathematical entities whose existence depend on the Axiom of Choice (and statements about those entities) are the usual examples of non-constructive notions in Mathematics, and he aimed his approach to incorporate constructivity at some level. In this paper we have proceed with this line of research and we introduced a restricted class of Kolgomorov problems, which we call *Veloso Problems*, and we have shown that if we restrict ourselves to this class and assume that the presented machinery holds in full generality then we get, again, equivalences of the Axiom of Choice. We have also shown that some related/restricted notions on problems are intrinsically associated to weak choice principles such as the Axiom of Countable Choice and the Principle

of Dependent Choices. To determine precisely the deductive strength of assertions relating to Kolgomorov and Veloso problems (positioning them in the hierarchy of weak choice principles) seems to deserve further research, and the same could be said about the following question:

Question 5.1 (implicit in [22])**.** *How to deal with the above mentioned non-constructive aspects of Kolgomorov-Veloso theory of problems within constructive environments?*

The work in this paper shows that some answers to this question are obtained by focusing on *relations*, instead of *functions*. In fact, equivalences with choice principles arise from assuming either the existence of solution functions (Theorems 3.12, 3.14 and 3.15) or of solution sequences (Theorem 3.19).

Veloso (op.cit.) presents some arguments against the use of relations instead of functions in the representation of solutions of problems. He argues that if the solution of a problem can be represented as a relation, then the problem condition itself, σ, would be a solution of the problem, and so nothing more would need to be done; to know the specification of the problem would solve it automatically. Second, he argues that, if one wants to assume that some instance $z \in I$ could be solved by more than one element of the set of possible solutions S then, even in this case, it is possible to work with a representation using functions, but in this case one should work with the so-called *multifunctions*, or multivalued functions. If I is the set of instances and S is the set of possible solutions of a viable problem P, a multifunction solution f would be, formally, a function with domain I and codomain $\mathcal{P}(S)$ (i.e, the set of all subsets of S) such that, for every $z \in I$, $f(z)$ is the *subset* of S given by $\{s \in S : z\,\sigma\,s\}$ – that is, the use of multivalued solution functions consists in associating each instance $z \in I$ to the set of *all* of its particular solutions.

Replying to the first argument, in practical applications, to know the *definition* of the condition problem σ does not give a solution automatically (even less the set of all solutions) for an instance $z \in I$. In simple/naive cases, the more realistic approach would be, probably, to proceed with some decision problem/search problem considering, for each $z \in I$, the set $\{z\} \times S$ as a domain and with $(\{z\} \times S) \cap \sigma$ as the set of yes-instances for this problem. So, to know the problem condition does not solve the problem. For instance, one may consider the viable problem $(\{\zeta\}, \mathbb{C}, \sigma)$, on which ζ is Riemann's zeta function and σ is the relation given by $\zeta\,\sigma\,c \iff \zeta(c) = 0$ – that is, σ is the restriction to $\{\zeta\}$ of the very general problem of finding zeros of analytic functions. Despite σ being perfectly (and easily) defined, we still do not know (after more than 150 years, see [3]) whether there are complex numbers (apart from the even negative numbers) with real part distinct from $\frac{1}{2}$ which solve the problem.

For the second objection against relations as solutions, we would like to mention two points. The first is that, if we decide to work with the powerset $\mathcal{P}(S)$ instead of S, then we are dramatically increasing the cardinality of the sets we are dealing with. For problems where any instance has only a *finite* set of solutions there is perhaps no major issue but we want to work with theories where problems have instances with possible infinite solutions. (Actually the set-theory applications do insist on infinite sets.) As some features of the theory may depend on the cardinalities of the constituents of the triples of the corresponding categories (as in the definitions of $\mathcal{PV}$ and $\mathcal{PV}_X$ for a given infinite set X, see Definitions 3.1 and 3.2), it would not be desirable such a dramatic increase in cardinality. The second argument is that if we assume $f(z)$ to be the set of all solutions (for f a multivalued solution function and z some instance of the problem) then we have all solutions for z "locked inside a box"; these solutions may become individually inaccessible and this precludes a qualitative analysis of them. We prefer to have the possibility of comparing distinct solutions for any fixed instance of the problem we are solving. Thus we insist that relations are a better modelling tool than functions, one that allows us to move on to functions, when and if we feel **AC** is adequate.

A second main conclusion for us is that the notions of reduction between problems, considered by Kolmogorov, Veloso and Blass, seen to be well modelled by the categorical morphisms in either $\mathrm{Dial}_2(\mathbf{Sets})$, its dual or the original dialectica construction. A skeptical reader may complain that the categorical language used is not buying us much. We beg to differ: the possibility of relating formally these, to begin with, quite 'woolly' notions of problems and solutions, seems a serious step forward in the hard task of detecting unwarranted foundational assumptions that tend to 'sneak' into mathematics. We still need to investigate whether the traditional tools of category theory, e.g. products, coproducts, exponentials, (co-)limits, etc. can be leveraged to our advantage. And, apart of such traditional tools, we are also interested in the investigation of the possible interactions between the Dialectica categorical modelling of problems and the so-called *lenses* ([7], [21]). Lenses are constructions used in situations where some structure is converted to different forms – through actions and observations between environments and agents – in such a way that all changes made can be reflected as updates to the original structure. Such constructions have attracted the attention of several researchers over the past ten years (see also [14], and references therein).

A possible avenue for further work from this point on would be to connect the categorical semantics meaning of $\mathrm{Dial}_2(\mathbf{Sets})$ (logically speaking $\mathrm{Dial}_2(\mathbf{Sets})$ models Linear Logic, together with Intuitionistic Propositional Logic) to, yet to be conceived, models of Ecumenical Propositional Logic. Ecumenical Propositional Logic [17] is Prawitz' recent suggestion of how to consider under the same umbrella both intuitionsitic and classical principles, as used by mathematicians. Since both Kolmogorov and Veloso mentioned their intentions of being understood by both classical and intuitionistic mathematicians, it would be extremely nice if the categorical models discussed here could help with modelling ecumenical logic. However new insights will be required to deal with the traditional issues of modelling categorically classical logic.

Acknowledgements. The authors would like to thank Professor Andreas Blass for the seminal article that was the original source of our joint research project [20]. We would also like to thank Professor Wagner Sanz for, not only calling our attention to Veloso's work in the 80's, but also for providing us with the necessary means to comparing our work to his own. His presentation [18] at the online seminar "Logicians in Quarantine" (sponsored by the Brazilian Logic Society and by the Interest Group on Logic of the Brazilian Computing Society) during the COVID-19 pandemics was our starting point. Thus we would like to thank the organizers of these splendid seminars as well.

References

[1] Charles E. Blair. The Baire category theorem implies the principle of dependent choices. *Bull. Acad. Pol. Sci., Sér. Sci. Math. Astron. Phys.*, 25:933–934, 1977.

[2] Andreas Blass. Questions and answers—a category arising in linear logic, complexity theory, and set theory. *Advances in linear logic*, 222:61–81, 1995.

[3] Enrico Bombieri. The Riemann Hypothesis: Official Problem Description. Clay Mathematics Institute, 2008, pp.1–5.

[4] Valeria C.V. de Paiva. The dialectica categories. In *Categories in Computer Science and Logic, Proceedings of a Summer Research Conference, held June 14–20, 1987 (eds J. Gray and A Scedrov)*, pages 23–47. American Mathematical Society, 1989.

[5] Conal Elliott. The simple essence of automatic differentiation. *Proceedings of the ACM on Programming Languages*, 2(ICFP):1–29, 2018.

[6] Jean-Yves Girard. Linear logic. *Theoretical computer science*, 50(1):1–101, 1987.

[7] Jules Hedges. Lenses for philosophers. Blog post, https://julesh.com/2018/08/16/lenses-for-philosophers, Aug 2016.

[8] Paul Howard and Jean E. Rubin. *Consequences of the axiom of choice.*, volume 59. Providence, RI: American Mathematical Society, 1998.

[9] R. Impagliazzo and L. A. Levin. No better ways to generate hard np instances than picking uniformly at random. In *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science*, pages 812–821 vol.2, 1990.

[10] Andrei Kolmogorov. On the interpretation of intuitionistic logic. *Selected Works of A.N. Kolmogorov, Volume 1, AMthematics and Mechanics, ed. V. M. Tikhomirov*, 1991.

[11] Per Martin-Löf. 100 years of Zermelo's axiom of choice: what was the problem with it? *The Computer Journal*, 49(3):345–350, 02 2006.

[12] Gregory H. Moore. Zermelo's axiom of choice. Its origins, development and influence. Studies in the History of Mathematics and Physical Sciences, 8. New York - Heidelberg - Berlin: Springer-Verlag. XIV, 410 pp., 1982.

[13] Justin Moore, Michael Hrušák, and Mirna Džamonja. Parametrized $\diamondsuit$ principles. *Transactions of the American Mathematical Society*, 356(6):2281–2306, 2004.

[14] nLab authors. lens (in computer science). Blog post, https://ncatlab.org/nlab/show/lens+(in+computer+science), jul 2020. Revision 11.

[15] Valeria de Paiva. A dialectica-like model of linear logic. In D. Pitt, D. Rydeheard, P. Dybjer, A. Pitts, and A. Poigne, editors, *Category Theory and Computer Science*, pages 341–356. Springer, 1989.

[16] Valeria de Paiva. *The Dialectica Categories*. Computer Laboratory, University of Cambridge, 1991.

[17] Elaine Pimentel, Luiz Carlos Pereira, and Valeria de Paiva. An ecumenical notion of entailment. *Synthese*, pages 1–23, 2019. https://doi.org/10.1007/s11229-019-02226-5.

[18] Wagner Sanz. Kolgomorov and the general theory of problems. To appear in a Volume dedicated to Prof. Dr. Peter Schröeder-Heister (Tübingen).

[19] Samuel G. da Silva. The Axiom of Choice and the Partition Principle from Dialectica Categories. *Logic Journal of the IGPL*, to appear, 2020.

[20] Samuel G. da Silva and Valeria C. V. de Paiva. Dialectica categories, cardinalities of the continuum and combinatorics of ideals. *Logic Journal of the IGPL*, 25(4):585–603, 06 2017.

[21] David I. Spivak. Lenses: applications and generalizations. Talk at the Special Session on Applied Category Theory, AMS Western Sectional Meeting, Riverside, Nov 2019.

[22] Paulo Veloso. Aspectos de uma teoria geral de problemas. *Cadernos de História e Filosofia da Ciência*, 7:21–42, 1984.

[23] R. Venkatesan and L. A. Levin. Random instances of a graph coloring problem are hard. In *STOC '88: Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 217–222, 1988.

[24] Peter Vojtáš. Generalized Galois-Tukey-connections between explicit relations on classical objects of real analysis. In *Set theory of the reals. Proceedings of a winter institute on set theory of the reals held at Bar-Ilan University, Ramat-Gan (Israel), January 1991*, pages 619–643. Providence, RI: American Mathematical Society (Distrib.); Ramat-Gan: Bar-Ilan University, 1993.