On the Conditions for Domain Stability for Machine Learning: a Mathematical Approach

Gabriel Pedroza
[0000−0002−7889−2892]

Ansys, France
gabriel.pedroza@ansys.com, pedrozafm@gmail.com
www.linkedin.com/in/gabriel-pedroza-89bb5338

Abstract. This work proposes a mathematical approach that (re)defines a property of Machine Learning models named stability and determines sufficient conditions to validate it. Machine Learning models are represented as functions, and the characteristics in scope depend upon the domain of the function, what allows us to adopt topological and metric spaces theory as a basis. Finally, this work provides some equivalences useful to prove and test stability in Machine Learning models. The results suggest that whenever stability is aligned with the notion of function smoothness, then the stability of Machine Learning models primarily depends upon certain topological, measurable properties of the classification sets within the ML model domain.

Keywords: Machine Learning, Classifiers, Stability, Operational Design Domain, Metric/Topological Spaces

1 Introduction

In recent years, the study of Artificial Intelligence and related techniques, like Machine Learning, has attracted considerable attention from practitioners, engineers and researchers from many sectors. Such interest has been, in many respects, driven by questions and concerns raised and shared by the involved communities. In particular, it can be mentioned the need for safety of systems integrating AI algorithms and the possibility to achieve acceptable means for compliance, necessary for regulation and certification [3][2][1]. Despite autonomy is a well-known notion within the Systems, SW and HW engineering arenas, the usage of AI technology, (GenAI, LLMs, ML/DL) to carry out functions traditionally conducted under human supervision and control, induces new challenges [4]. Discussing referred challenges is out of the scope of this paper: notwithstanding the relevance of AI challenges and risks, they are currently under inspection and study by a variety of experts, following a plethora of approaches, ranging from conceptual to empirical/pragmatical [5][10]. From the variety and heterogeneity of those studies, a consensus seems to emerge: despite the significant advances in AI technology, a considerable amount of requirements and properties still need to be ensured for the AI systems to be trustworthy and aligned with requirements. It is known that the lack of properties like robustness, generalization, and stability in ML models can have impacts at different system levels [11]. Several authors even highlight a lack of methods to validate and ensure referred properties [7]. In addition, the observed uncertainty of ML performance raise questions on the foundations of the AI algorithms. A basis for their sound design and validation seems necessary but still missing. This work aims to provide a preliminary mathematical basis to analyze ML models abstracted as functions. It mainly introduces a property named stability, which appears to be fundamental for ML classification. This preliminary work provides some equivalences which can be useful to prove stability. Topological and metric spaces [6][9] were adopted as foundation to conduct this work which also relies on the theory of functional analysis [8].

2 Defining Stability

Definition 1. *Let (S, d) a metric space, $D_i \subset S$, $i = 1 \dots m$, a finite sequence of sets. M is a classifier on S for the sets $\{D_i\}$ if:*

i) *M is a function defined on $\bigcup_{i=1}^{m} D_i$*
ii) $D_i \cap D_j = \emptyset$, $\forall i \neq j$
iii) $\exists y_i \in M(D_i)$, $\forall x \in D_i \Rightarrow M(x) = y_i, \quad i = 1 \dots m$
iv) *For $y_i, \ y_j$ as in previous point, if $i \neq j \ \Rightarrow \ y_i \neq y_j$*

Note 1. Given a metric space (S, d) the following notation is used for the neighborhood of a point $x_o \in S$:

$$B(x_o, \delta) = \{x \in S \mid d(x_o, x) < \delta\}$$

Note 2. In Definition 1, a point $x \in D_i$, $M(x) = y_i$ is denoted by x_{y_i}. The assignation $M(x_{y_i}) = y_i$ can also be denoted by $x_{y_i} \xmapsto{M} y_i$.

Definition 2. *Let (S, d) a metric space, $D \subset S$ and M a classifier for D and D^c. $x_y \in D$ is said a stable point of M in D if it is satisfied:*

i) $M(x_y) = y$
ii) $\exists \delta > 0, \ \forall x \in B(x_y, \delta) \Rightarrow x \in D, \ M(x) = y$
iii) *For δ as in point ii), $\forall \delta_\alpha \leq \delta \ \exists x \in B(x_y, \delta_\alpha)$, $x \neq x_y$*

Practically, the existence of stable points for a classifier M implemented in a programming language, relies upon the limited/finite precision of computers. Indeed, the precision of a machine can be approximated, for instance, by an iterative algorithm taking $\varepsilon_o > 0$ as input and computing $\varepsilon_{n+1} = \varepsilon_n/2^n$ at each iteration n. The stopping criterion is when $1 + \varepsilon_n = 1$. Then, a candidate for δ is any number $k-$times bigger than ε_n. i.e. $\delta := k\varepsilon_n$.
The Definition 2 helps to identify cases where classifiers are unable to smoothly classify subsets within its domain, as can be seen in the following example.

Example 1. Let M be a classifier in the interval $S = [0, 1]$, with the 1-euclidean metrics for the sets $D_1 = \mathbb{I} \cap S$ and $D_2 = \mathbb{Q} \cap S$. Given that D_1 and D_2 are dense, then the set of stable points of M in D_i is empty.

3 Dense sets and Implications for Stability

The implications of dense sets regarding the existence (absence) of stable points is formalized in this subsection.

Definition 3. *Let (S, d) a metric space. A set $D \subset S$ is said dense in S if $\forall x \in S$, $\forall \delta > 0$, $B(x, \delta) \cap D \neq \emptyset$ [9], [6].*

Lemma 1. *Let (S, d) a metric space and M a classifier for $D \subset S$ and D^c. If D^c is dense in S then the set of stable points in D is empty.*

First, $S = D \cup D^c$. Let's assume $x_o \in D$ a stable point of M, then $\exists \delta > 0$ such that $B(x_o, \delta) \subset D$. Since D^c is dense in S, then $B(x_o, \delta) \cap D^c \neq \emptyset$. However, if $x \in B(x_o, \delta) \cap D^c$ then $x \in D^c$ and by definition 2, *ii)* $x \in D$ what contradicts the assumption. QED.

By exchanging roles between D and D^c in previous lemma, the following corollary is proved.

Corollary 1. *Let (S, d) a metric space and M a classifier for $D \subset S$ and D^c. If D is dense, then D^c does not have any stable point.*

Corollary 2. *Let $S \subset \mathbb{R}$ a (non-empty) interval, then there is no classifier M able to classify $S \cap \mathbb{I}$ and $S \cap \mathbb{Q}$.*

Indeed, since $(S \cap \mathbb{Q}) = (S \cap \mathbb{I})^c$ and $S \cap \mathbb{I} = (S \cap \mathbb{Q})^c$ are both dense, by lemma 1 and Corollary 1 the conclusion follows. QED.

The previous results, which hold particularly for intervals in $\mathbb{R}$, are generalized in the following lemma.

Lemma 2. *Let (S, d) a metric space and M a classifier for a collection of sets $D_1 \ldots D_n \subset S$ such that $S = \cup_{i=1}^{n} D_i$. If there is D_k dense in S then there is no stable point for M in any of the sets D_i for $i \neq k$.*

Let's assume there is $x_j \in S$ such that $x_j \in D_j,\ j \neq k$, is a stable point for M. Then $M(x_j) = j$ and $\exists\delta > 0$ such that $B(x_j, \delta) \subset D_j$. However, since D_k is dense in S, then $B(x_j, \delta) \cap D_k \neq \emptyset$. Then for any point $x \in B(x_j, \delta) \cap D_k$, it occurs that $M(x) = j$ and $M(x) = k$, and $x \in D_j \cap D_k$ which contradicts Definition 1 *i*), *ii*), *iv*) and Definition 2, *ii*). QED.

4 Alternatives to Prove Stability

Some equivalences are provided as alternatives to prove stability.

4.1 Accumulation Points

Definition 4. *Let (S, d) a metric space. Given a set $D \subset S$, a point $x \in S$ is an accumulation point of D if $\forall\delta > 0$ then $B(x, \delta) \cap D \backslash \{x\} \neq \emptyset$ [9] [6].*

Lemma 3. *Let (S, d) a metric space and M a classifier for D and D^c, with both D and D^c not dense in S and D an open set. Then $x_y \in D$ is a stable point for M if and only if x_y is an accumulation point of D.*

[$\Rightarrow$]
Let's assume $x_y \in D$ is a stable point of M. It will be proved that x_y is an accumulation point of D.
Let's consider $\varepsilon > 0$ arbitrary but fixed. Then since $x_y \in D$ is a stable point of M, $M(x_y) = y$ and $\exists\delta > 0$ such that $B(x_y, \delta) \subset D$ and $\forall\delta_\alpha \leq \delta$, $\exists x \in B(x_y, \delta_\alpha),\ x \neq x_y$. The following cases exist:

If $\varepsilon < \delta$: then $B(x_y, \varepsilon) \subset B(x_y, \delta) \subset D$, since $\exists x \in B(x_y, \varepsilon),\ x \neq x_y$, it follows that $x \in D$, which leads directly to $B(x_y, \varepsilon) \cap D \backslash \{x_y\} \neq \emptyset$.

If $\varepsilon > \delta$: since $x_y \in D$ is stable point of M, then $\exists x \in B(x_y, \delta) \subset B(x_y, \varepsilon)$, $x \neq x_y$ and $x \in D$, what also leads to $B(x_y, \varepsilon) \cap D \backslash \{x_y\} \neq \emptyset$.

[$\Leftarrow$]
Now, let's assume x_y is an accumulation point of D, an open set. It will be proved that $x_y \in D$ is a stable point of M.

By definition, $\forall \delta > 0,\ B(x_y, \delta) \cap D \backslash \{x_y\} \neq \emptyset$. Let $\delta > 0$ arbitrary but fixed. Then, since $\forall \delta_\alpha \leq \delta,\ B(x_y, \delta_\alpha) \cap D \backslash \{x_y\} \neq \emptyset$, this implies that $\exists x_\alpha \in B(x_y, \delta_\alpha) \cap D,\ x_\alpha \neq x_y$. Therefore, $M(x_\alpha) = y$ since $x_\alpha \in D$ and M classifier for D and D^c. Previous statement holds for any $\delta_\alpha \leq \delta$. Let's assume $\forall \delta_\alpha < \delta,\ B(x_y, \delta_\alpha) \cap D^c \neq \emptyset$. Since D is open and $x_y \in D$, then $\exists \varepsilon > 0$ such that $B(x_y, \varepsilon) \subset D$. The following cases exist:

If $\varepsilon < \delta$: then $B(x_y, \varepsilon) \subset D$ and $B(x_y, \varepsilon) \cap D^c \neq \emptyset$ what is a contradiction

If $\varepsilon > \delta$: then $B(x_y, \delta) \subset B(x_y, \varepsilon) \subset D$, what conflicts with the assumption $\forall \delta_\alpha < \delta,\ B(x_y, \delta_\alpha) \cap D^c \neq \emptyset$

Therefore $\exists \delta_\alpha < \delta$ such that $B(x_y, \delta_\alpha) \cap D^c = \emptyset$ what implies $B(x_y, \delta_\alpha) \subset D$, thus $\forall x \in B(x_y, \delta_\alpha) \ \Rightarrow M(x) = y$. QED.

4.2 Accumulation series

As shown in previous subsection, a classifier M defined over an open set is stable for every accumulation point therein. The equivalence provided in the following lemma provides further means to prove stability.

Lemma 4. *Let (S, d) a metric space and M a classifier for D and D^c, with both D and D^c not dense in S and D an open set. x_y is a stable point of M if and only if $\forall \{x_n\}$ series, such that $lim_{n \to \infty} x_n = x_y,\ x_n \neq x_y$, $\exists \{s_k\}$ sub-series of $\{x_n\}$ such that $\exists k_o,\ k \geq k_o, \Rightarrow s_k \in D,\ s_k \neq x_y$, $lim_{k \to \infty} s_k = x_y$.*

[$\Rightarrow$]
Let's assume x_y is a stable point of M. Let $\{x_n\}$ be a series such that $lim_{n \to \infty} x_n = x_y,\ x_n \neq x_y$, then $\exists \delta > 0$ such that $B(x_y, \delta) \subset D$. For such δ, $\exists n_o$ such that $\forall n > n_o,\ d(x_y, x_n) < \delta$, what means that $\forall n > n_o,\ x_n \in B(x_y, \delta) \subset D$, then $M(x_n) = y,\ x_n \neq x_y$. Then, we can define the sub-series of $\{x_n\}$ as $\{s_k\} = \{x_n\} \cap B(x_y, \delta) \cap D \backslash \{x_y\} \neq \emptyset$. Thus, by its construction, $\{s_k\}$ satisfies $\exists k_o,\ k \geq k_o, \Rightarrow s_k \in D,\ s_k \neq x_y$, $lim_{k \to \infty} s_k = x_y$.

[$\Leftarrow$]
Let $\delta > 0$. Then, if $lim_{n\to\infty} x_n = x_y$, $x_n \neq x_y$, and $\exists\{s_k\}$ a sub-series of $\{x_n\}$ such that $\exists k_o,\ k \geq k_o, \Rightarrow s_k \in D,\ s_k \neq x_y,\ lim_{k\to\infty} s_k = x_y$, let $\varepsilon = d(s_{k_o}, x_y)$. The following cases exist:

If $\varepsilon < \delta$: $\forall k > k_o, \Rightarrow s_k \in B(x_y, \varepsilon) \subset B(x_y, \delta)$ and $s_k \in D,\ s_k \neq x_y$, therefore $\forall k > k_o,\ s_k \in D \cap B(x_y, \delta) \backslash \{x_y\} \neq \emptyset$.

If $\varepsilon > \delta$: since $lim_{k\to\infty} s_k = x_y$, then for the given δ, $\exists k_1$ such that $\forall k \geq k_1,\ d(x_y, s_k) < \delta$. If $k_2 = max\{k_o, k_1\}$, then $\forall k > k_2,\ s_k \in B(x_y, \delta) \subset B(x_y, \varepsilon)$ and $s_k \in D,\ s_k \neq x_y$, therefore $\forall k > k_2,\ s_k \in D \cap B(x_y, \delta) \backslash \{x_y\} \neq \emptyset$.

Thus, in any case x_y is an accumulation point. Then by lemma 3, the conclusion follows. QED.

5 Discussion

Machine Learning models and their respective implementations include some uncertainties due to singularity regions. As such, the abstraction provided in this paper named classifier (Definition 1) is indeed a rough approximation of ML models. Nonetheless, the results obtained mostly rely upon properties of the domain of the ML model and not in the classifier itself. An important claim in this approach is that the conditions for ML stability depend, in a first place, upon certain topological and measurable properties of the space, namely density, accumulation and openness. Overall, open and bounded sets are suitable candidates sets for stable classification. As it is shown, if such topological/metric properties are not ensured, classifiers cannot ensure a stable operation. This approach shall be leveraged, by adapting the notion of classifier so as to consider the uncertainty of classifiers. This is left as a future work. The equivalence between stability and the so named accumulation series is intended to facilitate the specification of algorithms to test (absence of) stability. Whereas accumulation points and the density of sets are simple notions, they can be hard to verify on complex, high dimension domains. Then the notion of accumulation series seeks for a discrete solution, more adapted to finite/limited precision of computers. A description of such discrete algorithms was barely sketched but not formally defined.

6 Conclusions

This work aims to provide further understanding regarding foundational aspects of Machine Learning models. The first part of this paper introduces a definition for stability, a property that appears fundamental for the proper operation of classifiers which are defined as a function that abstracts the uncertainty of real Machine Learning models. Secondly, some limits of classifiers were explained which appear whenever one or more classification sets are dense. Indeed, it was proved that the stability of classifiers demands the absence of dense sets in the domain of classification (also called Operational Design Domain) (Lemmas 1, 2). Some basic but representative examples were provided to illustrate such limitations. The last part of this work provides alternatives to prove stability in the form of equivalences: Lemma 3 provides conditions for equivalence between stability and accumulation points, then, Lemma 4 proves the equivalence between accumulation points and so named accumulation series, also introduced in this paper. The resulting equivalence between stability and accumulation series provides the possibility to define finite, discrete algorithms to prove stability. The definition of referred algorithms is not included in this paper and will be addressed as a continuation of this work.

References

1. Confiance.AI Project: The Confiance.AI Project (2024), https://www.confiance.ai/
2. DEEL Project: Dependable, Certifiable & Explainable Artificial Intelligence for Critical Systems (2024), https://www.deel.ai/
3. European Commission: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (2024), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206
4. Fischer, L., Ehrlinger, L., Geist, V., Ramler, R., Sobieczky, F., Zellinger, W., Brunner, D., Kumar, M., Moser, B.: Ai system engineering—key challenges and lessons learned. Machine Learning and Knowledge Extraction **3**, 56–83 (12 2020). https://doi.org/10.3390/make3010004
5. Habbal, A., Ali, M.K., Abuzaraida, M.A.: Artificial intelligence trust, risk and security management (ai trism): Frameworks, applications, challenges and future research directions. Expert Systems with Applications **240**, 122442 (2024)
6. Halmos, P.R.: Measure Theory. Springer New York, NY (1974), https://link.springer.com/book/10.1007/978-1-4684-9440-2
7. Harel, D., Marron, A., Sifakis, J.: Autonomics: In search of a foundation for next-generation autonomous systems. Proceedings of the National Academy of Sciences **117**(30), 17491–17498 (jul 2020)
8. Lang, S.: Real and Functional Analysis. Springer New York, NY (1993), https://link.springer.com/book/10.1007/978-1-4612-0897-6

9. Lee, J.M.: Introduction to Topological Manifolds. Springer New York, NY (2010), `https://link.springer.com/book/10.1007/978-1-4419-7940-7`
10. Piorkowski, D., Hind, M., Richards, J.: Quantitative ai risk assessments: Opportunities and challenges. arXiv preprint arXiv:2209.06317 (2022)
11. Tan, W.G.Y., Wu, Z.: Robust machine learning modeling for predictive control using lipschitz-constrained neural networks. Computers & Chemical Engineering **180**, 108466 (2024)