
Specifying and Testing k -Safety Properties for Machine-Learning Models

Maria Christakis
MPI-SWS
Germany
maria@mpi-sws.org

Hasan Ferit Eniser
MPI-SWS
Germany
hfeniser@mpi-sws.org

Jörg Hoffmann
Saarland University, Saarland Informatics Campus
German Research Center for Artificial Intelligence (DFKI)
Germany
hoffmann@cs.uni-saarland.de

Adish Singla
MPI-SWS
Germany
adishs@mpi-sws.org

Valentin Wüstholtz
ConsenSys
Germany
valentin.wustholz@consensys.net

Abstract

Machine-learning models are becoming increasingly prevalent in our lives, for instance assisting in image-classification or decision-making tasks. Consequently, the reliability of these models is of critical importance and has resulted in the development of numerous approaches for validating and verifying their robustness and fairness. However, beyond such specific properties, it is challenging to specify, let alone check, general functional-correctness expectations from models. In this paper, we take inspiration from specifications used in formal methods, expressing functional-correctness properties by reasoning about k different executions—so-called k -safety properties. Considering a credit-screening model of a bank, the expected property that "if a person is denied a loan and their income decreases, they should still be denied the loan" is a 2-safety property. Here, we show the wide applicability of k -safety properties for machine-learning models and present the first specification language for expressing them. We also operationalize the language in a framework for automatically validating such properties using metamorphic testing. Our experiments show that our framework is effective in identifying property violations, and that detected bugs could be used to train better models.

1 Introduction

Due to the impressive advances in machine learning and the unlimited availability of data, machine-learning (ML) models, *e.g.*, neural networks, are rapidly becoming prevalent in our lives, for instance by assisting in image-classification or decision-making tasks. As a result, there is growing concern about the reliability of these models in performing such tasks. For example, it could be disastrous if an autonomous vehicle misclassifies a street sign, or if a recidivism-risk algorithm, which predicts whether a criminal is likely to re-offend, is unfair with respect to race. The research community is, of course, aware of these issues and has devised numerous techniques to validate and verify robustness and fairness properties of machine-learning models (*e.g.*, [18, 14, 31, 1, 2, 37, 5, 15, 24, 13, 36, 35]).

Beyond such specific properties however, it is challenging to express general functional-correctness expectations from such models, let alone check them, *e.g.*, how can we specify that an image classifier should label images correctly? We take inspiration from specifications used in formal methods—so-called *hyperproperties* [8]—capturing functional-correctness properties by simultaneously reasoning about multiple system executions. For example, consider a credit-screening model of a bank. The expected property that "if a person is denied a loan and their income decreases, they should still be denied the loan", or conversely "if a person is granted a loan and their income increases, they should still be granted the loan", is a *2-safety* hyperproperty—we need two model executions to validate its correctness. In contrast, the property that "a person with no income should be denied a loan" is a standard (1-)safety property since it can be validated by individual model executions. Overall, *k-safety hyperproperties* generalize standard safety properties in that they require reasoning about *k* different executions.

Examples. To demonstrate the wide applicability of *k-safety* properties for ML models, we use examples from five distinct domains throughout this paper:

- *Tabular data.* Consider the COMPAS dataset [20], which determines how likely criminals are to re-offend. An expected hyperproperty for models trained on COMPAS could be that "if the number of committed felonies for a given criminal increases, then their recidivism risk should not decrease". Note that this is essentially monotonicity in an input feature, a special case of the hyperproperties we consider here.
- *Images.* Using the MNIST dataset [21], which classifies images of handwritten digits, an expected hyperproperty could be that "if a blurred image is correctly classified, then its unblurred version should also be correctly classified". Note that this is *not* monotonicity in a feature as whether or not an image is blurred does not constitute part of the model input (*i.e.*, the image); instead, blurring may affect most, if not all, pixels.
- *Speech.* Similarly, for the SpeechCommand dataset [42], which classifies short spoken commands, an expected hyperproperty could be that "if a speech command with white noise is correctly classified, then its non-noisy version should also be correctly classified".
- *Natural language.* The HotelReview dataset [22] is used for sentiment analysis of hotel reviews. An expected hyperproperty could be that "if a review becomes more negative, then the sentiment should not become more positive". Note that, again, making a review more negative may significantly affect the model input.
- *Action policies.* LunarLander is a popular Gym [4] environment consisting of a 2D-world with an uneven lunar surface and a reinforcement-learning (RL) lander, which initially appears far above the surface and moves downward. The goal is to navigate and land the lander on its two legs; if the body ever touches the surface, the lander crashes. An expected hyperproperty could be that "if the lander lands successfully, then decreasing the surface height (thus giving the lander more time to land) should also result in landing successfully". Here, even a seemingly simple change to the initial game state may result in significant changes to subsequent states since the policy is invoked repeatedly during the game.

Note that, in practice, such properties are defined by users, thus expressing model expectations that are deemed important in their particular usage scenario.

Related work. There is work on expressing *k-safety* properties for programs [32], but no prior work has explored how to specify such properties for ML models and how to leverage these specifications for automated testing. Numerous techniques verify specific functional-correctness properties of models, such as robustness (*e.g.*, [18, 14, 31, 3, 40]), fairness (*e.g.*, [1, 2, 37]), and others (*e.g.*, [19, 39]). There are also approaches for validating such properties (*e.g.*, [5, 15, 24, 13, 36, 35]). Although certain popular robustness and fairness properties do, in fact, constitute 2-safety properties (*e.g.*, slightly perturbing the pixels of an image should not change its classification, or changing the race of a criminal should not make them more or less likely to re-offend), none of this work targets general hyperproperties. The most relevant work is by Sharma and Wehrheim [30], who introduce verification-based testing of monotonicity in ML models. As indicated above, a model is said to be monotone with respect to an input feature if an increase in the feature implies an increase in the model's prediction, *e.g.*, the higher the income, the larger the loan. In addition, Deng et al. [10, 9] propose an approach for testing image-based autonomous-vehicle models against safety properties defined in domain-specific behaviour templates that resemble natural language.

Approach and contributions. In this paper, we show the wide applicability of k -safety properties for ML models. We design a declarative, domain-agnostic specification language, NOMOS ("law" in Greek), for writing them. In contrast to existing approaches, NOMOS can express general k -safety properties capturing *arbitrary* relations between more than one input-output pair; these subsume the more specific relations of robustness, fairness, and monotonicity. Going a step further, we design a fully automated framework for validating NOMOS properties using *metamorphic testing* [7, 29]. On a high-level, our framework takes as input the model under test and a set of k -safety properties for the model. As output, it produces test cases for which the model violates the specified properties. Note that a single test case for a k -safety property consists of k concrete inputs to the model under test. Under the hood, the *harness generator* component of the framework compiles the provided NOMOS properties into a *test harness*, *i.e.*, software that tests the given model against the properties. The harness employs a *test generator* and an *oracle* component, for generating inputs to the model using metamorphic testing and for detecting property violations, respectively.

In summary, this paper makes the following key contributions:

- We present NOMOS, the first specification language for expressing general k -safety hyperproperties for ML models.
- We demonstrate the wide applicability of such properties through case studies from several domains and the expressiveness of our language in capturing them.
- We design and implement a fully automated framework for validating such properties using metamorphic testing.
- We evaluate the effectiveness of our testing framework in detecting property violations across a broad range of different domains. We also perform a feasibility study to showcase how such violations can be used to improve model training.

2 NOMOS Specification Language

NOMOS allows a user to specify k -safety properties over source code invoking an ML model under test. On a high level, a NOMOS specification consists of three parts: (1) the *precondition*, (2) the source code—Python in our implementation—invoking the model, and (3) the *postcondition*. Pre- and postconditions are commonly used in formal methods, for instance, in Hoare logic [16] and design by contract [25]. Here, we adapt them for reasoning about ML models and k -safety properties.

The precondition captures the conditions under which the model should be invoked, allowing the user to express arbitrary relations between more than one model input. It is expressed using zero or more `requires` statements, each capturing a condition over inputs; the logical conjunction of these conditions constitutes the precondition. The source code may be arbitrary code invoking the model one or more times to capture k input-output pairs. Finally, the postcondition captures the safety property that the model is expected to satisfy. It is expressed using zero or more `ensures` statements, each taking a condition that, unlike for the precondition, may refer to model outputs; the logical conjunction of these conditions constitutes the postcondition.

Examples. As an example, consider the NOMOS specification of Fig. 1a expressing the COMPAS property described earlier. On line 1, we specify that we need an input `x1`, *i.e.*, a criminal. Lines 2–4 get the first feature of `x1`, which corresponds to the number of felonies, and assign it to variable `v1`; in variable `v2`, we increase this number, and create a new criminal `x2` that differs from `x1` only with respect to this feature, *i.e.*, `x2` has committed more felonies than `x1`. Line 5 specifies a precondition that the new criminal’s felonies should not exceed a sensible limit. Lines 6–7 declare two outputs, `d1` and `d2`, that are assigned the model’s prediction when calling it with criminal `x1` and `x2`, respectively (see block of Python code on lines 8–11). Finally, on line 13, we specify the postcondition that the recidivism risk of criminal `x2` should not be lower than that of `x1`.

Fig. 1b shows the MNIST specification. Given an image `x1` (line 1), image `x2` is its blurred version (line 2), and variable `v1` contains its correct label (line 3), *e.g.*, retrieved from the dataset. Note that functions such as `blur` and `label` extend the core NOMOS language and may be easily added by the user. The postcondition on line 10 says that if the blurred image is correctly classified, then so should the original image. Note that we defined a very similar specification for the SpeechCommand property—instead of `blur`, we used function `wNoise` adding white noise to audio.

```

1 input x1;
2 var v1 := getFeat(x1, 1);
3 var v2 := v1 + randint(1, 10);
4 var x2 := setFeat(x1, 1, v2);
5 requires v2 <= 20;
6 output d1;
7 output d2;
8 {
9   d1 = predict(x1)
10  d2 = predict(x2)
11 }
12 # 0-low, 1-medium, 2-high risk
13 ensures d1 <= d2;

```

(a) COMPAS 2-safety hyperproperty.

```

1 input x1;
2 var x2 := blur(x1);
3 var v1 := label(x1);
4 output d1;
5 output d2;
6 {
7   d1 = predict(x1)
8   d2 = predict(x2)
9 }
10 ensures d2==v1 ==> d1==v1;

```

(b) MNIST 2-safety hyperproperty.

```

1 input x1;
2 input x2;
3 var v1 := getFeat(x1, 1);
4 var v2 := getFeat(x2, 1);
5 var v3 := strConcat(v1, v2);
6 var x3 := setFeat(x1, 1, v3);
7 output d1;
8 output d3;
9 {
10  d1 = predict(x1)
11  d3 = predict(x3)
12 }
13 # 0-pos, 1-neg
14 ensures d1 <= d3;

```

(c) HotelReview 2-safety hyperproperty.

```

1 input s1;
2 var s2 := relax(s1);
3 output o1;
4 output o2;
5 {
6   o1, o2 = 0, 0
7   for _ in range(10):
8     rs = randint(0, MAX_INT)
9     o1 += play(s1, rs)
10    o2 += play(s2, rs)
11 }
12 # 0-lose, 1-win
13 ensures o1 <= o2;

```

(d) LunarLander 20-safety hyperproperty.

Figure 1: Example k -safety specifications in NOMOS.

The HotelReview specification is shown in Fig. 1c. Note that a hotel review consists of a positive and a negative section, where a guest describes what they liked and did not like about the hotel, respectively. On lines 1–2, we obtain two reviews, x_1 and x_2 , and in variables v_1 and v_2 on lines 3–4, we store their negative sections (feature 1 retrieved with function `getFeat`). We then create a third review, x_3 , which is the same as x_1 except that its negative section is the concatenation of v_1 and v_2 (lines 5–6). The postcondition on line 14 checks that the detected sentiment is not more positive for review x_3 than for x_1 .

Finally, consider the LunarLander specification in Fig. 1d. On line 1, we obtain an input s_1 , which is an initial state of the game. Line 2 “relaxes” this state to obtain a new state s_2 , which differs from s_1 only in that the height of the lunar surface is lower. In the block of Python code that follows (lines 5–11), we initialize outputs o_1 and o_2 to zero and play the game from each initial state, s_1 and s_2 , in a loop; o_1 and o_2 accumulate the number of wins. We use a loop because the environment is stochastic—firing an engine of the lander follows a probability distribution. Therefore, by changing the environment random seed rs on line 8, we take stochasticity into account. In each loop iteration however, we ensure that the game starting from s_2 is indeed easier, *i.e.*, that stochasticity cannot make it harder, by using the same seed on lines 9–10. Note that function `play` invokes the policy multiple times (*i.e.*, after every step in the game simulator). Finally, line 13 ensures that, when playing the easier game (starting with s_2), the number of wins should not decrease. Since this property depends on 20 model invocations, it is a 20-safety property! Conversely, we can also make the game harder by “unrelaxing” the original initial state, *i.e.*, increasing the surface height. In such a case, when playing the harder game, the number of wins should not exceed the original number of wins.

Grammar. Fig. 2 provides a formal grammar for NOMOS (in a variant of extended Backus-Naur form). The top-level construct is `<spec>` on lines 1–2. It consists of zero or more `import` statements—the curly braces denote repetition—to import source-code files containing custom implementations for domain-specific functions, *e.g.*, `blur` or `wNoise`, one or more input declarations,

```

1 <spec> ::= { <import> } <input> { <input> } { <var_decl> } { <precond> }
2 { <output> } "{" <code> "}" { <postcond> }
3 <import> ::= "import" <model_name> ";"
4 <input> ::= "input" <var_name> ";"
5 <var_decl> ::= "var" <var_name> ":" <scalar_expr> ";"
6 | "var" <var_name> ":" <record_expr> ";"
7 <precond> ::= "requires" <bool_expr> ";"
8 <output> ::= "output" <var_name> ";"
9 <postcond> ::= "ensures" <bool_expr> ";"
10 <scalar_expr> ::= <bool_expr>
11 | <int_expr>
12 | <string_expr>
13 | "getFeat(" <record_expr> ", " <int_expr> ")"
14 | "label(" <record_expr> ")"
15 | "randInt(" <int_expr> ", " <int_expr> ")"
16 | "strConcat(" <string_expr> ", " <string_expr> ")"
17 <bool_expr> ::= <bool_literal>
18 | <var_name>
19 | "!" <bool_expr>
20 | <bool_expr> "&&" <bool_expr>
21 | <scalar_expr> "==" <scalar_expr>
22 | <scalar_expr> "<" <scalar_expr>
23 | <record_expr> "==" <record_expr>
24 <record_expr> ::= <var_name>
25 | "setFeat(" <record_expr> ", " <int_expr> ", " <scalar_expr> ")"
26 | "blur(" <record_expr> ")"
27 | "wNoise(" <record_expr> ")"
28 | "relax(" <record_expr> ")"
29 | "unrelax(" <record_expr> ")"

```

Figure 2: The NOMOS grammar.

variable declarations, preconditions, output declarations, the source-code block, and postconditions. We define these sub-constructs in subsequent rules (lines 4–9). For instance, a precondition (line 7) consists of the token `requires`, a Boolean expression, and a semicolon. For brevity, we omit a definition of `<code>`; it denotes arbitrary Python code that is intended to invoke the model under test and assign values to output variables. We also omit the basic identifiers `<model_name>` and `<var_name>`.

The grammar additionally defines various types of expressions needed in the above sub-constructs. In their definitions, we use the `|` combinator to denote alternatives. In particular, we define scalar (lines 10–16), Boolean (lines 17–23), and record expressions (lines 24–29). The latter are used to express complex object-like values, such as images or game states. In these definitions, we include extensions to the core language with domain-specific functions that support the application domains considered in this paper—e.g., `getFeat` and `setFeat` retrieve and modify record fields, respectively. Integer and string expressions are defined as expected (see appendix), and we omit the basic scalar expressions `<bool_literal>`, `<int_literal>`, and `<string_literal>`.

3 Metamorphic-Testing Framework for NOMOS Specifications

Metamorphic testing [7, 29] is a testing technique that addresses the lack of an existing *oracle* defining correct system behavior. Specifically, given an input, metamorphic testing transforms it such that the relation between the outputs (*i.e.*, the output of the system under test when executed on the original input and the corresponding output when executed on the transformed input) is known. If this relation between outputs does not actually hold, then a bug is detected. As a simple example, consider testing a database system; given a query as the original input, assume that the transformed input is the same query with weakened constraints. A bug is detected if the transformed query returns fewer results than the original one, which is more restrictive. So far, metamorphic testing has been used to test ML models from specific application domains, *e.g.*, image classifiers [11, 34], translation systems [38], NLP models [23], object-detection systems [41], action policies [12], and autonomous cars [33, 43].

In our setting, we observe that metamorphic testing is a natural choice for validating general k -safety properties as these also prescribe input transformations and expected output relations. For instance, in Fig. 1a, lines 2–5 describe the transformation to input x_1 in order to obtain x_2 , and line 13 specifies the relation between the corresponding outputs. We, therefore, design the framework in Fig. 3 for validating a model against a NOMOS specification using metamorphic testing. The output of our

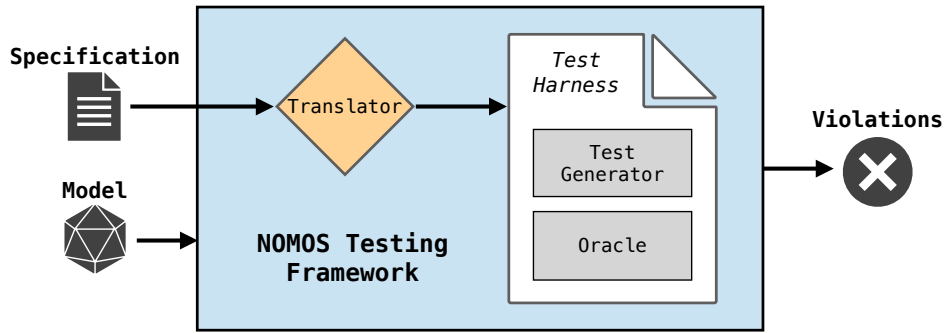


Figure 3: An overview of our testing framework.

framework is a set of (unique) bugs, *i.e.*, test cases revealing postcondition violations. For Fig. 1a, a bug would comprise two concrete instances of a criminal, c_1 and c_2 , such that (1) c_2 differs from c_1 only in having more felonies, and (2) the recidivism risk of c_2 is predicted to be lower than that of c_1 .

Under the hood, the *harness generator* component of the framework compiles the NOMOS specification into a *test harness*, *i.e.*, a Python program that tests the model against the specified properties. Our implementation parses NOMOS specifications using an ANTLR4 [26] grammar. After semantically checking the parsed abstract syntax tree (AST), our framework translates the AST into the Python program constituting the test harness. A snippet of the generated harness for the specification of Fig. 1a is shown in Fig. 4. The test harness employs a *test generator* and an *oracle* component, for generating inputs to the model using metamorphic testing and for detecting postcondition violations, respectively.

As shown in Fig. 4, the model is tested until a user-specified budget is depleted (line 1). In each iteration of this loop, the test generator creates k model inputs that satisfy the given precondition, if any (lines 3-11). Specifically, for every `input` declaration, the test generator randomly selects an input from a source specified in the imported files (line 4)—note that `import` statements are not shown here but are defined on line 3 of Fig. 2. In our evaluation, we have used both the test set and the output of an off-the-shelf fuzzer [12] as such input sources. The metamorphic transformation of an input can be performed through `var` declarations, which are compiled into temporary variables in the harness (lines 5-7). Before the test generator returns the k generated model inputs, the specified precondition is checked; if it is violated, the process repeats until it holds (lines 9-11).

Next, the block of Python code in the specification is executed (lines 12-14), and finally the oracle component checks the postcondition (lines 16-21). On line 21, the oracle records each detected bug and processes it for subsequent de-duplication. In particular, for each bug, the oracle hashes any source of randomness in generating the model inputs (*i.e.*, for the example of Fig. 4, there is randomness on lines 4 and 6). Two bugs are considered duplicate if their hashes match, that is, if the

```

1 while budget > 0:
2
3     # test generator
4     x1 = compas.randInput()
5     v1 = compas.getFeat(x1,1)
6     v2 = v1 + compas.randint(1,10)
7     x2 = compas.setFeat(x1,1,v2)
8
9     if not(v2 <= 20):
10        compas.precond_violtn += 1
11        continue
12
13     # code
14     d1 = compas.predict(x1)
15     d2 = compas.predict(x2)
16
17     # oracle
18     if d1 <= d2 :
19         compas.passed += 1
20     else:
21         compas.postcond_violtn += 1
22         compas.process_bug()
23         budget -= 1

```

Figure 4: Snippet of generated harness for the specification of Fig. 1a.

Table 1: Number of specified properties, violated properties, and unique bugs per dataset and model.

Dataset	Model	Properties		Unique Bugs
		Specified	Violated	
COMPAS	NN	12	7	960.0
	DT	12	6	294.8
GermanCredit	NN	10	6	295.2
	DT	10	6	286.9
MNIST	NN	1	1	22.4
SpeechCommand	NN	1	1	14.2
HotelReview	NN	4	4	3288.0
LunarLander	RL	2	2	3459.0

generated model inputs are equivalent. Note that we avoid comparing model inputs directly due to their potential complexity, *e.g.*, in the case of game states.

4 Experimental Evaluation

So far, we have demonstrated the expressiveness of NOMOS by specifying hyperproperties for models in diverse domains. This section focuses on evaluating the effectiveness of our testing framework in finding bugs in these models. We describe the benchmarks, experimental setup, and results. We also present a feasibility study on how detected bugs can be used to improve model training.

Benchmarks. We trained models using six datasets from five application domains as follows:

- *Tabular data.* We used the COMPAS [20] and GermanCredit [17] datasets, which we pre-process. For each dataset, we trained a fully connected neural network (NN) and a decision tree (DT). For COMPAS, we achieved 74% (NN) and 72% (DT) accuracy, and for GermanCredit, 78% (NN) and 70% (DT). Note that, even though we report accuracy here, the achieved score does not necessarily affect whether a specified property holds, *i.e.*, a perfectly accurate model could violate the property, whereas a less accurate model might not.
- *Images.* Using the MNIST dataset [21], we trained a fully connected neural network achieving 97% accuracy.
- *Speech.* We pre-processed the SpeechCommand dataset [42] to convert waveforms to spectrograms, which show frequency changes over time. As spectrograms are typically represented as 2D-images, we trained a convolutional neural network classifying spectrogram images. The model achieves 84% test accuracy.
- *Natural language.* For the HotelReview dataset [22], we used a pre-trained Universal Sentence Encoder (USE) [6] to encode natural-language text into high dimensional vectors. USE compresses any textual data into a vector of size 512 while preserving the similarity between sentences. We trained a fully connected neural network of 82% accuracy on the encoded hotel reviews.
- *Action policies.* In LunarLander [4], touching a leg of the lander to the surface yields reward +100, whereas touching the body yields -100; the best-case reward is over 200. We trained an RL policy that achieves an average reward of 175 (after 1 million training episodes).

Experimental setup. For each of these models, we wrote one or more NOMOS specifications to capture potentially desired properties (see appendix for a complete list). Each test harness used a budget of 5000 (see line 1 of Fig. 4), that is, it generated 5000 test cases satisfying the precondition, if any. We ran each harness with 10 different random seeds to account for randomness in the testing procedure. Here, we report arithmetic means (*e.g.*, for the number of bugs) unless stated otherwise. In all harnesses except for LunarLander, the input source (*e.g.*, line 4 of Fig. 4) is the test set. In the LunarLander harness, the input source is a pool of game states that was generated by π -fuzz [12] after fuzzing our policy for 2 hours.

Results. We specified 30 properties across all datasets. Tab. 1 provides an overview of the number of specified properties, violated properties, and unique bugs per dataset and model. Our testing framework was able to find violations for all datasets, and in particular, for 24 of these properties.

Table 2: Minimum-bug and maximum-reward policies generated with normal and guided training.

Minimum-Bug Policy				Maximum-Reward Policy			
Normal		Guided		Normal		Guided	
Bugs	Rew.	Bugs	Rew.	Bugs	Rew.	Bugs	Rew.
19	230.8	19	242.0	27	232.0	23	261.5
12	155.5	7	160.1	16	157.2	8	197.0
20	257.0	12	254.4	32	277.3	16	279.0
19	170.2	19	170.2	29	175.0	27	184.5
28	83.7	16	62.9	29	137.2	34	167.7
8	237.4	6	208.9	11	243.6	13	256.2
21	224.8	12	254.7	29	240.8	21	264.1
17	15.0	7	220.2	24	181.7	12	221.6
14	263.5	9	209.0	14	263.5	23	242.4
9	128.1	2	144.4	16	158.7	7	217.0

Most property violations were exhibited through tens or hundreds of unique tests. This demonstrates that our framework is effective in detecting bugs even with as few as 5000 tests per property; in contrast, fuzzers for software systems often generate millions of tests before uncovering a bug.

The average number of bugs per property varies significantly depending on the property, model, and dataset (see appendix for details). For instance, for COMPAS, the average number of bugs ranges from 0.5 to 619.7 when testing the NN classifier against each of the twelve different properties.

There are six properties that were not violated by any model trained on the COMPAS and German-Credit datasets. For four of these properties, we observed that the involved features almost never affect the outcome of our models, thereby trivially satisfying the properties. In the remaining cases, the training data itself seems to be sufficient in ensuring that the properties hold for the models.

Feasibility study. Our results show that our framework is effective in detecting property violations. But are these violations actionable? A natural next step is to use them for repairing the model under test or incorporate them when training the model from scratch—much like adversarial training for robustness issues. While a comprehensive exploration and discussion of such options is beyond the scope of this work, we did perform a feasibility study to investigate whether the reported violations are indeed actionable.

For this study, we selected LunarLander due to its higher complexity. On a high level, we incorporated buggy game states, *i.e.*, ones that resulted in property violations, during policy training. In particular, we adjusted the existing training algorithm (PPO [28] implemented in the SB3 library [27]) to start episodes not only from random initial states, but also from buggy states. As training progresses, our guided-training algorithm gradually increases the probability of starting from buggy states. The intuition behind this choice is to focus more on "ironing out" bugs toward the end of the training, when the policy is already able to achieve decent rewards.

Under the hood, our guided-training algorithm tests the current policy at regular intervals (every 5 rollouts in our experiments), essentially alternating between training and testing phases. Any bugs that are found during the latest testing phase are added to a pool of buggy states from which the algorithm selects initial states during subsequent training phases. Note that we prioritize most recently detected buggy states, but we also include older bugs to ensure the policy does not "forget" later on.

For our experiments, we trained 10 policies with each training algorithm, *i.e.*, normal and guided. Tab. 2 summarizes the policies that were generated during these training runs—each row corresponds to a training run. In the four leftmost columns, we focus on policies with the fewest number of bugs. The first two columns show the number of bugs and reward for the minimum-bug policy generated during each of the normal-training runs. Note that, for policies with the same number of bugs during a run, we show the one with higher reward. Similarly, the third and fourth columns show the same data for guided training. In the four rightmost columns, we focus on policies with the highest reward. Again, for policies with the same reward, we show the one with fewer bugs.

Looking at the first and third columns, no normal-training run achieves fewer bugs than the corresponding guided-training run, and guided training results in fewer bugs in 8 out of 10 runs. Looking

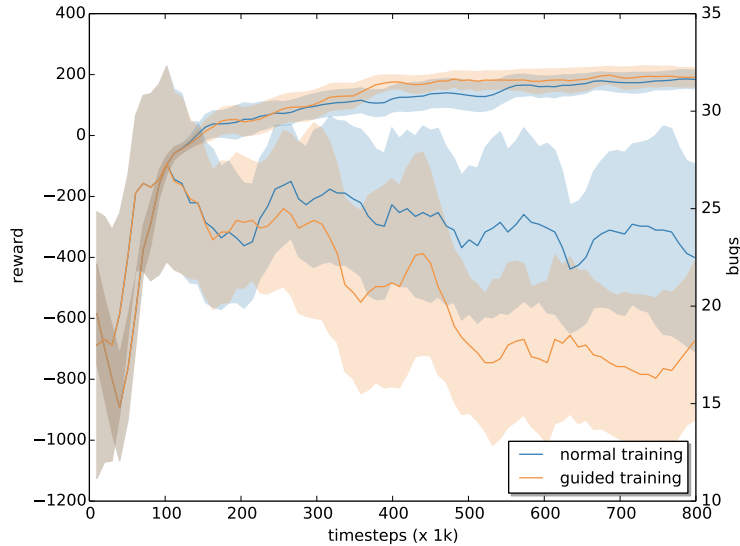


Figure 5: Increase in reward and decrease in number of bugs over time for normal and guided training.

at the second and fourth columns, guided training does not result in significantly lower rewards for the minimum-bug policies; in 5 out of 10 runs, guided minimum-bug policies surpass, in terms of reward, the corresponding normal policies. In addition, when looking at the fourth and sixth columns, 4 out of 10 guided minimum-bug policies even surpass the normal maximum-reward policies. Similarly, when considering the maximum-reward policies, guided training results in higher rewards in 9 out of 10 runs; in 7 runs, guided policies have fewer bugs; and 4 guided maximum-reward policies have fewer bugs than the corresponding normal minimum-bug policies.

Fig. 5 shows the increase in reward and decrease in number of bugs over time both for normal and guided training. The dark lines represent the mean values, and the lighter shaded areas denote the 90% confidence interval. As expected, we observe that, for guided training, the number of bugs is consistently lower without compromising on the achieved reward.

Overall, our experiments show that property violations can be useful not only for assessing the quality of a model, but also for training better models. The latter is a promising direction for future work.

5 Conclusion and Outlook

We have presented the NOMOS language for specifying k -safety properties of ML models and an automated testing framework for detecting violations of such properties. NOMOS is the first high-level specification language for expressing general hyperproperties of models, subsuming more specific ones such as robustness and fairness. We have demonstrated the wide applicability of such properties through case studies from several domains and evaluated the effectiveness of our framework in detecting property violations. Although users could manually write test cases or a test harness for each desired property, this would be tedious, repetitive, and easy to get wrong; it would also be difficult to update and extend properties if needed. In contrast, our NOMOS specifications are concise and enable users to think about properties on a higher level of abstraction.

There are several promising directions for future work. For the ML community, model repair and guided training might be the most interesting direction for building on NOMOS and our testing framework. One way to think about specifications is as a, possibly infinite, source of training examples. Our feasibility study has already provided some empirical evidence for how such examples can be incorporated in the training process. However, more work is needed, and adversarial-training techniques could be adapted to improve the effectiveness.

For the testing community, an interesting direction could be to explore more effective input-generation techniques, such as coverage-guided testing. This may reduce the testing time or increase the number

of bugs that can be found within a given time budget. Such advances can be crucial for reducing the testing overhead when performing guided training.

For the formal-methods community, a natural next step is to build verification tools for certifying that a property holds *for all inputs*. This could be particularly promising for models that are used in safety-critical domains, such as autonomous driving.

We believe that NOMOS can bring these communities together to facilitate the development of functionally correct ML models.

References

- [1] Aws Albarghouthi, Loris D’Antoni, Samuel Drews, and Aditya V. Nori. FairSquare: Probabilistic verification of program fairness. *PACMPL*, 1:80:1–80:30, 2017.
- [2] Osbert Bastani, Xin Zhang, and Armando Solar-Lezama. Probabilistic verification of fairness properties via concentration. *PACMPL*, 3:118:1–118:27, 2019.
- [3] Leonard Berrada, Sumanth Dathathri, Krishnamurthy Dvijotham, Robert Stanforth, Rudy Bunel, Jonathan Uesato, Sven Gowal, and M. Pawan Kumar. Make sure you’re unsure: A framework for verifying probabilistic specifications. In *NeurIPS*, pages 11136–11147, 2021.
- [4] Greg Brockman, Vicki Cheung, Ludwig Pettersson, Jonas Schneider, John Schulman, Jie Tang, and Wojciech Zaremba. OpenAI Gym. *CoRR*, abs/1606.01540, 2016.
- [5] Nicholas Carlini and David A. Wagner. Towards evaluating the robustness of neural networks. In *S&P*, pages 39–57. IEEE Computer Society, 2017.
- [6] Daniel Cer, Yinfei Yang, Sheng-yi Kong, Nan Hua, Nicole Limtiaco, Rhomni St. John, Noah Constant, Mario Guajardo-Cespedes, Steve Yuan, Chris Tar, Yun-Hsuan Sung, Brian Strope, and Ray Kurzweil. Universal sentence encoder. *CoRR*, abs/1803.11175, 2018.
- [7] Tsong Yueh Chen, S. C. Cheung, and Siu-Ming Yiu. Metamorphic testing: A new approach for generating next test cases. Technical Report HKUST-CS98-01, HKUST, 1998.
- [8] Michael R. Clarkson and Fred B. Schneider. Hyperproperties. In *CSF*, pages 51–65. IEEE Computer Society, 2008.
- [9] Yao Deng, Guannan Lou, James Xi Zheng, Tianyi Zhang, Miryung Kim, Huai Liu, Chen Wang, and Tsong Yueh Chen. BMT: Behavior driven development-based metamorphic testing for autonomous driving models. In *MET@ICSE*, pages 32–36. IEEE Computer Society, 2021.
- [10] Yao Deng, Xi Zheng, Tianyi Zhang, Guannan Lou, Huai Liu, and Miryung Kim. RMT: Rule-based metamorphic testing for autonomous driving models. *CoRR*, abs/2012.10672, 2020.
- [11] Anurag Dwarakanath, Manish Ahuja, Samarth Sikand, Raghotham M. Rao, R. P. Jagadeesh Chandra Bose, Neville Dubash, and Sanjay Podder. Identifying implementation bugs in machine learning based image classifiers using metamorphic testing. In *ISSTA*, pages 118–128. ACM, 2018.
- [12] Hasan Ferit Eniser, Timo P. Gros, Valentin Wüstholtz, Jörg Hoffmann, and Maria Christakis. Metamorphic relations via relaxations: An approach to obtain oracles for action-policy testing. In *ISSTA*. ACM, 2022. To appear.
- [13] Sainyam Galhotra, Yuriy Brun, and Alexandra Meliou. Fairness testing: Testing software for discrimination. In *ESEC/FSE*, pages 498–510. ACM, 2017.
- [14] Timon Gehr, Matthew Mirman, Dana Drachler-Cohen, Petar Tsankov, Swarat Chaudhuri, and Martin T. Vechev. AI2: Safety and robustness certification of neural networks with abstract interpretation. In *S&P*, pages 3–18. IEEE Computer Society, 2018.
- [15] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. In *ICLR*, 2015.
- [16] C. A. R. Hoare. An axiomatic basis for computer programming. *CACM*, 12:576–580, 1969.
- [17] Hans Hofmann. The German credit dataset. [https://archive.ics.uci.edu/ml/datasets/Statlog+\(German+Credit+Data\)](https://archive.ics.uci.edu/ml/datasets/Statlog+(German+Credit+Data)).
- [18] Xiaowei Huang, Marta Kwiatkowska, Sen Wang, and Min Wu. Safety verification of deep neural networks. In *CAV*, volume 10426 of *LNCS*, pages 3–29. Springer, 2017.

- [19] Guy Katz, Clark W. Barrett, David L. Dill, Kyle Julian, and Mykel J. Kochenderfer. Reluplex: An efficient SMT solver for verifying deep neural networks. In *CAV*, volume 10426 of *LNCS*, pages 97–117. Springer, 2017.
- [20] Jeff Larson, Surya Mattu, Lauren Kirchner, and Julia Angwin. How we analyzed the COMPAS recidivism algorithm, 2016. <https://www.propublica.org/article/how-we-analyzed-the-compass-recidivism-algorithm>.
- [21] Yann LeCun, Corinna Cortes, and Christopher J.C. Burges. The MNIST database of handwritten digits. <http://yann.lecun.com/exdb/mnist>.
- [22] Jiashen Liu. 515K hotel reviews data in Europe. <https://www.kaggle.com/datasets/jiashenliu/515k-hotel-reviews-data-in-europe>.
- [23] Pingchuan Ma, Shuai Wang, and Jin Liu. Metamorphic testing and certified mitigation of fairness violations in NLP models. In *IJCAI*, pages 458–465. ijcai.org, 2020.
- [24] Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. Towards deep learning models resistant to adversarial attacks. In *ICLR*. OpenReview.net, 2018.
- [25] Bertrand Meyer. *Eiffel: The Language*. Prentice-Hall, 1992.
- [26] Terence Parr. *The Definitive ANTLR 4 Reference, 2nd Edition*. O’Reilly Media, 2013.
- [27] Antonin Raffin, Ashley Hill, Maximilian Ernestus, Adam Gleave, Anssi Kanervisto, and Noah Dormann. Stable baselines3, 2019. <https://github.com/DLR-RM/stable-baselines3>.
- [28] John Schulman, Filip Wolski, Prafulla Dhariwal, Alec Radford, and Oleg Klimov. Proximal policy optimization algorithms. *CoRR*, abs/1707.06347, 2017.
- [29] Sergio Segura, Gordon Fraser, Ana B. Sánchez, and Antonio Ruiz Cortés. A survey on metamorphic testing. *TSE*, 42:805–824, 2016.
- [30] Arnab Sharma and Heike Wehrheim. Higher income, larger loan? Monotonicity testing of machine learning models. In *ISSTA*, pages 200–210. ACM, 2020.
- [31] Gagandeep Singh, Timon Gehr, Markus Püschel, and Martin T. Vechev. An abstract domain for certifying neural networks. *PACMPL*, 3:41:1–41:30, 2019.
- [32] Marcelo Sousa and Isil Dillig. Cartesian Hoare logic for verifying k-safety properties. In *PLDI*, pages 57–69. ACM, 2016.
- [33] Yuchi Tian, Kexin Pei, Suman Jana, and Baishakhi Ray. DeepTest: Automated testing of deep-neural-network-driven autonomous cars. In *ICSE*, pages 303–314. ACM, 2018.
- [34] Yuchi Tian, Ziyuan Zhong, Vicente Ordonez, Gail E. Kaiser, and Baishakhi Ray. Testing DNN image classifiers for confusion & bias errors. In *ICSE*, pages 1122–1134. ACM, 2020.
- [35] Florian Tramèr, Vaggelis Atlidakis, Roxana Geambasu, Daniel J. Hsu, Jean-Pierre Hubaux, Mathias Humbert, Ari Juels, and Huang Lin. FairTest: Discovering unwarranted associations in data-driven applications. In *EuroS&P*, pages 401–416. IEEE Computer Society, 2017.
- [36] Sakshi Udeshi, Pryanshu Arora, and Sudipta Chattopadhyay. Automated directed fairness testing. In *ASE*, pages 98–108. ACM, 2018.
- [37] Caterina Urban, Maria Christakis, Valentin Wüstholtz, and Fuyuan Zhang. Perfectly parallel fairness certification of neural networks. *PACMPL*, 4:185:1–185:30, 2020.
- [38] Improving Machine Translation Systems via Isotopic Replacement. Sun, zeyu and zhang, jie m. and xiong, yingfei and harman, mark and papadakis, mike and zhang, lu. In *ICSE*. ACM, 2022. To appear.
- [39] Shiqi Wang, Kexin Pei, Justin Whitehouse, Junfeng Yang, and Suman Jana. Formal security analysis of neural networks using symbolic intervals. In *Security*, pages 1599–1614. USENIX, 2018.
- [40] Shiqi Wang, Huan Zhang, Kaidi Xu, Xue Lin, Suman Jana, Cho-Jui Hsieh, and J. Zico Kolter. Beta-CROWN: Efficient bound propagation with per-neuron split constraints for neural network robustness verification. In *NeurIPS*, pages 29909–29921, 2021.
- [41] Shuai Wang and Zhendong Su. Metamorphic object insertion for testing object detection systems. In *ASE*, pages 1053–1065. IEEE Computer Society, 2020.

- [42] Pete Warden. Speech commands: A dataset for limited-vocabulary speech recognition. *CoRR*, abs/1804.03209, 2018.
- [43] Mengshi Zhang, Yuqun Zhang, Lingming Zhang, Cong Liu, and Sarfraz Khurshid. DeepRoad: GAN-based metamorphic testing and input validation framework for autonomous driving systems. In *ASE*, pages 132–142. ACM, 2018.

A List of Appendices

Below, we provide a brief description of each section in the appendix.

- We provide additional grammar definitions in Appendix B.
- We include all NOMOS specifications for our case studies in Appendix C.
- We present additional details of our experimental results (*e.g.*, number of bugs for each specification) in Appendix D.
- We present additional details of our experimental setup (*e.g.*, details on model training and hardware setup) in Appendix E.

B Additional Grammar Definitions

Grammar definition for integer expressions in NOMOS:

```
1 <int_expr> ::= <int_literal>
2             | <var_name>
3             | "-" <int_expr>
4             | <int_expr> "+" <int_expr>
5             | <int_expr> "-" <int_expr>
6             | <int_expr> "*" <int_expr>
7             | <int_expr> "/" <int_expr>
```

Grammar definition for string expressions in NOMOS:

```
1 <string_expr> ::= <string_literal>
2             | <var_name>
```

We omit the basic scalar expressions `<int_literal>` and `<string_literal>`.

C Specifications

Below, we provide a description of each specified property:

Felony Inc If the number of committed felonies for a criminal increases, then their recidivism risk should not decrease.

Felony Dec If the number of committed felonies for a criminal decreases, then their recidivism risk should not increase.

Misdmnr Inc If the number of committed misdemeanors for a criminal increases, then their recidivism risk should not decrease.

Misdmnr Dec If the number of committed misdemeanors for a criminal decreases, then their recidivism risk should not increase.

Priors Inc If the number of priors for a criminal increases, then their recidivism risk should not decrease.

Priors Dec If the number of priors for a criminal decreases, then their recidivism risk should not increase.

Others Inc If the number of other crimes committed by a criminal increases, then their recidivism risk should not decrease.

Others Dec If the number of other crimes committed by a criminal decreases, then their recidivism risk should not increase.

IsRecid Set If a criminal becomes a recidivist, then their recidivism risk should not decrease.

IsRecid Unset If a criminal ceases to be a recidivist, then their recidivism risk should not increase.

IsVRecid Set If a criminal becomes a violent recidivist, then their recidivism risk should not decrease.

IsVRecid Unset If a criminal ceases to be a violent recidivist, then their recidivism risk should not increase.

Crdt Amount Inc If the credit amount requested by a person increases, then they should not be more likely to receive it.

Crdt Amount Dec If the credit amount requested by a person decreases, then they should not be less likely to receive it.

Crdt Hist Inc If a person’s credit history worsens, then they should not be more likely to receive credit.

Crdt Hist Dec If a person’s credit history improves, then they should not be less likely to receive credit.

Empl Since Inc If a person’s employment years increase, then they should not be less likely to receive credit.

Empl Since Dec If a person’s employment years decrease, then they should not be more likely to receive credit.

Install Rate Inc If a person’s installment rate (as a percentage of their disposable income) increases, then they should not be more likely to receive credit.

Install Rate Dec If a person’s installment rate (as a percentage of their disposable income) decreases, then they should not be less likely to receive credit.

Job Inc If a person is promoted, then they should not be less likely to receive credit.

Job Dec If a person is demoted, then they should not be more likely to receive credit.

Blur If a blurred image is correctly classified, then its unblurred version should also be correctly classified.

WNoise If a speech command with white noise is correctly classified, then its non-noisy version should also be correctly classified.

Pos-1 Deleting the positive comments of a hotel review should not make it more positive.

Pos-2 If more positive comments are added to a hotel review, it should not become more negative.

Neg-1 Deleting the negative comments of a hotel review should not make it more negative.

Neg-2 If more negative comments are added to a hotel review, it should not become more positive.

Relax If the lander lands successfully, then decreasing the surface height (thus giving the lander more time to land) should also result in landing successfully.

Unrelax If the lander fails to land, then increasing the surface height (thus giving the lander less time to land) should also result in failing to land.

D Additional Details of our Experimental Results

In this section, we provide more detailed results on the number of unique bugs for each individual specification.

The results for COMPAS are shown in Tab. 3. Column 2 shows the average number of unique bugs for the NN model and for each of the 12 specifications. Column 3 shows the same data for the DT model. For properties "IsRecid Set" and "IsRecid Unset", we observed that the involved feature "IsRecid" almost never affects the outcome of our models, thereby trivially satisfying the properties.

Tab. 4 shows similar results for GermanCredit. For properties "Install Rate Inc" and "Install Rate Dec", we observed that the involved feature "Installment Rate" almost never affects the outcome of our models, thereby trivially satisfying the properties.

Tab. 5 shows similar results for the remaining benchmarks.

E Additional Details of our Experimental Setup

E.1 Training Setup

For the COMPAS dataset, we trained a fully connected neural network and a decision tree classifier. The neural network is composed of 3 hidden layers of size 12, 9, and 9. We use the RMSprop

Table 3: Average number of unique bugs for each COMPAS specification.

Specification	Unique Bugs	
	NN	DT
Felony Inc	42.9	3.5
Felony Dec	0.0	0.0
Misdmmr Inc	619.7	0.0
Misdmmr Dec	4.0	0.0
Priors Inc	0.5	90.0
Priors Dec	0.0	97.2
Others Inc	289.0	91.1
Others Dec	3.0	8.0
IsRecid Set	0.0	0.0
IsRecid Unset	0.0	0.0
IsVRecid Set	0.9	5.0
IsVRecid Unset	0.0	0.0

Table 4: Average number of unique bugs for each GermanCredit specification.

Specification	Unique Bugs	
	NN	DT
Crdt Amount Inc	0.0	122.3
Crdt Amount Dec	0.0	75.4
Crdt Hist Inc	78.1	8.0
Crdt Hist Dec	122.8	31.2
Empl Since Inc	13.5	9.1
Empl Since Dec	30.9	40.9
Install Rate Inc	0.0	0.0
Install Rate Dec	0.0	0.0
Job Inc	47.9	0.0
Job Dec	2.0	0.0

algorithm for optimization. For decision-tree training, we set the *max_depth* parameter to 8. For training, we shuffle the data and use 67% of it.

For the GermanCredit dataset, we trained a fully connected neural network and a decision tree classifier. The neural network is composed of 1 hidden layer of size 10, and we use the Adam optimizer. In decision-tree training, we set the *max_depth* parameter to 6. For training, we shuffle the data and use 67% of it.

For the MNIST dataset, we trained a fully connected neural network consisting of 3 hidden layers (each with 30 neurons), and we use the Adam optimizer. We use the regular training set for training.

Table 5: Average number of unique bugs for all MNIST, SpeechCommand, HotelReview, and LunarLander specifications.

Benchmark	Specification	Unique Bugs
MNIST	Blur	22.4
SpeechCommand	WNoise	14.2
HotelReview	Pos-1	861.1
	Pos-2	876.1
	Neg-1	756.2
	Neg-2	794.6
LunarLander	Relax	124.5
	Unrelax	3334.5

For the SpeechCommand dataset, we apply a number of pre-processing steps and infer a spectrogram image for each audio file. We use 80% of the spectrogram inputs for training a convolutional neural network consisting of 2 convolutional layers with kernels (32x32x3) and (64x64x3), and a fully connected layer of size 128. We use dropout for regularization and Adam for optimization.

The HotelReview dataset consists of over 515k reviews, and only ca. 85k of them are scored above 6 (out of 10)—labeled as *positive* in our evaluation. We sample the same number of inputs from the ones that are labeled as *negative* to form a new dataset consisting of around 170k inputs. We use 90% of them as training set. We use the USE model from Tensorflow Hub¹. The USE-encoded reviews are used to train a fully connected neural network with 2 hidden layers (256 and 128 neurons, respectively). We use dropout for regularization and Adam for optimization.

For the LunarLander dataset, we use the default PPO implementation in the SB3 library for training the agent.

We use ReLU activation functions in all neural networks.

We use Tensorflow v2.7 and the scikit-learn v1.0.2 framework for training neural networks and decision trees, respectively.

E.2 Hardware Setup

We use a cluster with a Quadro RTX 8000 GPU and an Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz for training models and running tests. Running 5k tests takes a few seconds for decision trees. It takes longer for neural networks, ranging from 5 to 20 minutes depending on the specification and the dataset. For LunarLander, it takes up to 4 hours.

The total amount of compute for all experiments is ca. 1 day on the above cluster.

¹<https://tfhub.dev/google/universal-sentence-encoder-multilingual-large/3>