Blue Elephants Inspecting Pandas

Inspection and Execution of Machine Learning Pipelines in SQL

Maximilian E. Schüle
Technical University of Munich
m.schuele@tum.de

Alfons Kemper
Technical University of Munich
kemper@in.tum.de

Luca Scalerandi
Technical University of Munich
luca.scalerandi@tum.de

Thomas Neumann
Technical University of Munich
neumann@in.tum.de

ABSTRACT

Data preprocessing, the step of transforming data into a suitable format for training a model, rarely happens within database systems but rather in external Python libraries. Database systems are tuned for efficient data access and offer aggregate functions to calculate the distribution frequencies necessary to detect the under- or overrepresentation of a certain value within the data (bias).

We argue that database systems with SQL are capable of executing machine learning pipelines as well as discovering technical biases—introduced by data preprocessing—efficiently. Therefore, we present a set of SQL queries to cover data preprocessing and data inspection: During preprocessing, we annotate the tuples with an identifier to compute the distribution frequency of columns. To inspect distribution changes, we join the preprocessed dataset with the original one on the tuple identifier and use aggregate functions to count the number of occurrences per sensitive column. This allows us to detect operations which filter out tuples and thus introduce a technical bias even for columns preprocessing has removed. To automatically generate such queries, our implementation extends the mlinspect project to transpile existing data preprocessing pipelines written in Python to SQL queries, while maintaining detailed inspection results using views or common table expressions (CTEs). The evaluation proves that a modern beyond main-memory database system, i.e., Umbra, accelerates the runtime for preprocessing and inspection. Even PostgreSQL as a disk-based database system shows similar performance for inspection to Umbra when materialising views.

1 INTRODUCTION

A preprocessing pipeline is the connective link between the validated input data and the training of a model [12]. While a machine learning pipeline covers the entire life cycle of a model (see Figure 1), a data-preprocessing pipeline only refers to the part, which puts the available data into a form for training a machine learning model. Preprocessing consists of loading, joining, and filtering the data (step 1) and transforming existing columns or replacing missing values (step 2). Finally, the processed data is then fed into the model for training (step 3).

Data preprocessing alters the original data semantically, which can lead to the “over- or under-representation of a certain group” [8]. This is called a technical bias, when caused by data preprocessing, in contrast to a pre-existing bias already contained in the data. Technical biases that a static analysis of the pipeline cannot find are particularly critical. They occur after preprocessing has modified the data, for example, when a trained model frequently misclassifies some classes but works fine for others. Manually repeating and inspecting each step in a pipeline would be time-consuming for large datasets. Even if a technical bias is found, it has to be traced back to the bias-introducing operation to fix this data bug: Finding data bugs automatically would not only be interesting from a debugging perspective but also proactively ensure correctness and trustworthiness.

Programmatically inspecting intermediate results during execution reduces the effort to find technical biases. This includes counting the number of entries per group after each operation is performed to compute the ratio. The ratio is the relative distribution frequency of how often each sensitive group occurs within the data and should remain as constant as possible during preprocessing.

As the focus in machine learning lies on creating effective models and not on efficient data processing, the traditional wisdom is to use Python library functions not only for training a model...
but also for data preprocessing. However, database systems are tuned for efficient data access and manipulation [25, 31, 32]. In a relational database, a table out of columns (attributes) and tuples, which each is a set of attribute values, represents a dataset. A synthetic tuple identifier tid identifies a tuple and can be used to trace tuples throughout all operations. Database systems offer a declarative language, SQL, allowing the user to specify what to do rather than caring about optimisation details [43]. SQL provides aggregate functions that allow grouping by a column to count the number of occurrences per value that forms a sensitive group. Common table expressions (CTEs) allow us to modularise and to structure the SQL code [39]. Modularising the code causes no additional overhead since the database system’s query optimiser unnests nested subqueries before execution [21]. Moreover, modern database systems generate code for pipelined data processing [19, 38, 40, 44, 45]. This enables in-memory performance and eliminates the overhead of function calls and the need to materialise subresults. Thus, instead of delegating calls to library functions such as pandas, a database system will increase the overall performance of data preprocessing.

We argue that database systems with SQL are ideally suited for data inspection within machine learning pipelines. In our solution, one CTE/view represents one line of the original Python source code. We, therefore, present a set of SQL queries that cover the functionalities of certain Python libraries such as pandas and scikit-learn (see Figure 2). Furthermore, aggregate functions within CTEs/views will track the ratio for each group of interest to detect biases: We equip each tuple with a synthetic index (tid) to identify a tuple although the sensitive column is not part of the result. After each operation that influences the number of occurrences per tuple, e.g., joins or selections, the index allows the restoration of the sensitive column if needed to count the number of occurrences per group. This is the first study that allows inspection in SQL of columns not even present in the result by preserving the tid. To automatically generate these SQL queries, we extend the mlinspect framework [7, 8] with an SQL backend. This way we can rely on the user interface for bias detection but just generate the SQL queries in the background. Likewise, we are able to fall back on the original Python library function calls when no SQL substitute has been implemented so far. Generating SQL code from Python pipelines provides further advantages. Firstly, existing pipelines can benefit from the performance of database systems without alteration of the original code. Secondly, it allows a less verbose specification of pipelines, which is also accessible for those not too familiar with SQL. This study’s specific contributions are:

- inspection of preprocessing pipelines in SQL,
- a set of SQL expressions that cover the functionalities of the Python libraries pandas and scikit-learn,
- an SQL backend for the mlinspect framework to translate Python into SQL supporting many pandas and scikit-learn operations with a focus on inspection,
- an expandable transpilation framework\(^1\) to facilitate the addition of support for other libraries,
- executing the mlinspect inspection of pipelines while offloading all expensive computations to a database system,
- functionality to generate inspection-enabled SQL queries from pipelines written in Python without execution,
- full support for running and inspecting end-to-end pipelines including training and testing the models in Python.

\(^1\)https://github.com/tum-db/mlinspect4sql

This study comprises the following sections: Section 2 summarises the related work on debugging pipelines and SQL support for machine learning. Section 3 introduces the SQL expressions needed for tuple tracking and the detection of introduced biases. To generate these queries, Section 4 shows how to create an SQL backend for the mlinspect framework using monkey patching. This SQL backend further generates one CTE/view in SQL per line of the original Python code (Section 5). The evaluation in Section 6 presents the performance of selected pipelines within PostgreSQL and Umbra. Section 7 concludes this study with an outlook on further extensions.

2 RELATED WORK

This study combines research on integrating machine learning pipelines into database systems [1, 2, 5, 14, 27, 30, 48, 49, 53] with studies on debugging pipelines. Debugging machine learning pipelines is necessary to ensure fairness [23, 24, 26, 50, 51], when data transformations [29] introduce biases [13] or, more generally, to detect the cause of incorrect predictions. For example, SliceLine [28] proposes algorithms to investigate the effectiveness of training datasets. Breadcrumb [6] finds removed tuples in Spark. Vizier [3] is a debugging tool with SQL and Python integration that also uses Spark as backend. MLDebugger [17] and BugDoc [18] are data debuggers for VisTrails [4].

mlinspect [8] provides an extendable framework that, on the basis of declarative abstractions of popular data science libraries, allows insightful inspections without the need for manual code instrumentation. For these inspections, mlinspect mostly relies on the frameworks NumPy and pandas with mostly modest performance. mlinspect’s functionality for pipeline inspection does not require the alteration of any existing code. This work proposes SQL queries to perform the inspections recommended by mlinspect. The mlinspect project will form the basis for implementing
the proposed transpiling and offloading of data-intensive operations to a database system, including all inspection capabilities. Grizzly [10, 11] aims to replace the pandas library by transpiling Python code using pandas to SQL and offloading the operations to a database system. It is capable of dealing with external data, user-defined functions and reusing intermediate results. Grizzly can emit the generated SQL code but requires a connection to a database system to work in the first place, so we decided to generate the SQL queries independently. Furthermore, this work’s SQL code-generation covers data inspection and other library functions and stores each result in a view/CTE.

3 TUPLE-TRACKING AND INSPECTION

One contribution of this paper is the inspection of so-called data distribution bugs [8], which are based on pre-existing and introduced (technical) biases, when using SQL. A bias is a systematic error leading to irrational preferences or aversions [52]. There is no general recipe to avoid introducing a technical bias in data preprocessing prior to training a model but detection is possible. For bias detection, it is necessary to monitor the ratios per sensitive column, which is the distribution frequency of a value, and the introduced ratio changes after each operation.

Biases can also be induced for columns not present in the original data or such that preprocessing has removed. Tracking the tuples explicitly detects biases even when preprocessing has removed a sensitive column. To track tuples throughout the pipeline, it is necessary to cope with possible projections when the sensitive column is not part of the result. The proposed tuple tracking allows us to restore and monitor all columns present in the original data independently of their removal inside the pipeline. An example of a common projection is one-hot-encoding, where an input is turned into a binary array. Assigning a unique identifier to each entry allows ratio changes the pipeline has introduced independently of the tuple’s current representation to be discovered.

The mlinspect framework provides two checks: NoIllegalFeatures verifies that none of the used features in the provided dataset are contained in a blacklist of illegal feature names. NoBiasIntroducedFor targets pre-existing and technical biases.

The latter check is based on three inspections: MaterializeFirstOutputRows materialises a set of rows from the input by each operator, to easily examine the effects of the pipeline [8]. RowLineage provides lineage information for the resulting tuples. HistogramForColumns calculates the ratios for specified columns before and after each operation in the pipeline.

3.1 Tuple-Tracking and Inspection in SQL

To implement tuple tracking, an identifier for the tuples is needed. Most database systems allow access to the physical table location, which could be used as an identifier. For PostgreSQL, the ctid is such an identifier, although it is not suitable as a long-term identifier\(^2\). This is based on the possibility of garbage collection routines changing the physical location. As we extract the ctid, initially only once within a common table expression (Listing 1 lines 3-6), we ensure that we use consistent identifiers during the checks.

To reproduce mlinspect’s bias inspections in SQL, we need to compute and compare the ratios for each sensitive column (HistogramForColumns). In order to compare the ratios (Listing 1 lines 11-19), it is necessary to group by each sensitive column to count the initial and current number of occurrences per value. One common table expression retrieves the original number (Listing 1 lines 7f). When measuring the current number, there are two cases. In the simple case, the result table already contains the sensitive column. In this simple case, an aggregate function counts the number of occurrences per column directly (Listing 1 lines 9f). In the event that the current table contains the sensitive column, a join on the tuple identifier restores the requested column (Listing 2 lines 7-9). When an aggregation function is part of the preprocessing pipeline, the tuple identifiers must also be aggregated to form an array (Listing 3 line 5). Unnesting the array allows the number of included tuples (line 8) to be computed and the sensitive column to be restored if required.

3.2 Technical Bias Detection

Not all operations can introduce a bias, as not all operations add or remove tuples from the dataset. This section shows how a technical bias can be introduced but also how it can be detected. We want to inspect the columns race and age_group for an introduced bias. Lines 20 to 35 (Listing 4) contain operations that introduce a bias, for example, line 35 (see Figure 3). The projection in line 33 has removed the column age_group, so it is

---

\(^2\)https://www.postgresql.org/docs/12/ddl-system-columns.html
patients = pd.read_csv(os.path.join(str(get_project_root()),
    'example_pipelines', 'healthcare', 'patients.csv'),
na_values=?)

histories = pd.read_csv(os.path.join(str(get_project_root()),
    'example_pipelines', 'healthcare', 'histories.csv'),
na_values=?)
data = patients.merge(histories, on=["ssn"])
complications = data.groupby(["age_group"], agg={
    mean_complications: ('complications', 'mean')})
data = data.merge(complications, on='age_group')
data['label'] = 1 + data['mean_complications'] * 1.2

data = data[data['label'] > 0.25]
data['label'] = data['label'] * 2

data = data[['smoker', 'last_name', 'county',
    'num_children', 'race', 'income', 'label']]
data = data[data['county'] == (COUNTIES_OF_INTEREST)]


<table>
<thead>
<tr>
<th>county</th>
<th>race</th>
<th>age_group</th>
<th>Track_id_Patients</th>
<th>Track_id_Histories</th>
</tr>
</thead>
<tbody>
<tr>
<td>county_1</td>
<td>race_3</td>
<td>age_group_1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>county_2</td>
<td>race_2</td>
<td>age_group_2</td>
<td>2</td>
<td>23</td>
</tr>
<tr>
<td>county_3</td>
<td>race_2</td>
<td>age_group_1</td>
<td>3</td>
<td>33</td>
</tr>
<tr>
<td>county_2</td>
<td>race_2</td>
<td>age_group_2</td>
<td>4</td>
<td>44</td>
</tr>
<tr>
<td>county_1</td>
<td>race_1</td>
<td>age_group_1</td>
<td>5</td>
<td>55</td>
</tr>
<tr>
<td>county_1</td>
<td>race_1</td>
<td>age_group_2</td>
<td>6</td>
<td>66</td>
</tr>
</tbody>
</table>

Figure 3: Example of bias-introducing operation.

not explicitly present in the table and shown in grey. Apart from line 35, the joins in line 27 or 30 could introduce a bias as well depending on a join partner. If many people of one race live in a removed county, a racial bias will be introduced. Far less visible is that line 35 could also introduce a bias regarding the age_group. This seems contradictory, as the selection in line 33 has removed the column age_group. But biases can be introduced for columns not present in a dataset's current representation.

Before calculating the ratio changes for each group, one has to define the threshold for which a bias becomes unacceptable, for example 25%. If the representation of a feature in the data alters by more than or equal to 25%, it is assumed that the pipeline introduced a bias. Figure 4 presents the original ratio on the left and the new ratio on the right. The parentheses in the right table show the precise changes. The ratios can be calculated as described in Section 3.1 (Listing 1, 2). The ratios of the feature race did not surpass the threshold of 25% and are assumed acceptable. For the feature age_group, the changes for both classes changed by exactly 25%. In this case, age_group_2 is over- and age_group_1 is underrepresented, which could lead to a model discriminating against some groups if trained with this data.

CREATE TABLE patients_51_mlinid0 (
    "id" INT, "first_name" text,
    "last_name" text, "race" text, "county" text, num_children INT, income FLOAT, age_group text, ssn text);

COPY patients_51_mlinid0 ("id", "first_name", "last_name", "race", "county", num_children, income, "age_group", "ssn")
FROM 'patients.csv' WITH (DELIMITER ',', NULL '"', FORMAT CSV, HEADER TRUE);

CREATE TABLE histories_52_mlinid1 (
    "smoker" text, "complications" INT, "ssn" text);

COPY histories_52_mlinid1 ('smoker', 'complications', 'ssn')
FROM 'histories.csv' WITH (DELIMITER ',', NULL '"', FORMAT CSV, HEADER TRUE);

WITH patients_51_mlinid0_ctid AS (SELECT ctid AS patients_51_mlinid0_ctid FROM patients_51_mlinid0)
SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0_ctid

SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0

SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0

block_mlinid2_53 AS (SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0)

SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0

block_mlinid4_55 AS (SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0)

block_mlinid4_55 AS (SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0)

SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0

block_mlinid5_59 AS (SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0)

block_mlinid4_55 AS (SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0)

SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0

block_mlinid5_59 AS (SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0)

SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0

block_mlinid4_55 AS (SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0)

block_mlinid4_55 AS (SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0)

block_mlinid5_59 AS (SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0)

SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0

block_mlinid4_55 AS (SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0)

block_mlinid5_59 AS (SELECT * AS patients_51_mlinid0_ctid
FROM patients_51_mlinid0

WHERE 'county' IN ('county2', 'county3'))

SELECT * AS patients_51_mlinid0_ctid
FROM block_mlinid3_66

SELECT * AS patients_51_mlinid0_ctid
FROM block_mlinid3_66

SELECT * AS patients_51_mlinid0_ctid
FROM block_mlinid3_66

SELECT * AS patients_51_mlinid0_ctid
FROM block_mlinid3_66

GROUP BY 'age_group';

Listing 5: Inspection of column age_group in SQL.

3.3 Automated Inspection in SQL
To inspect the biases each time, mlinspect measures the column ratios, whereas our extension delegates the call instead to the database system, returns the measured results and injects them into the corresponding data class (SQLHistogramForColumns). At this point, the default functionality of mlinspect performs the comparison of the measured ratios to the user-given threshold. When a pre-defined threshold is exceeded, a bias has been introduced and the user is notified.

Listing 5 displays the translation of Listing 4 to SQL with inspection of the column age_group. The first lines (lines 1-4) import the tables from a CSV file. The first two CTExpose the ctid as a tuple identifier with a unique name (lines 6-11). Afterwards, one CTE represents one line of the original code, so either joins (lines 12-14, 18-20), an aggregation (lines 15-17), projections (lines 21-23, 24-26) or a condition (lines 27-29). Finally, lines 31-33 show the code to inspect the column age_group: First, the preserved ctid allows the reconstruction of this column as it was not part of the last projection. Then an aggregate function counts the number of occurrences per value, which is returned to the mlinspect framework.
3.4 User Interface for the SQL Target

Code-generation to SQL is realised as an extension to the mlinspect [8] project. The users alone are able to choose the right fit for the task at hand, so no functionality is forced on them. The changes do not duplicate existing functionality or require any later development on mlinspect to be altered. The goal is to translate a productive pipeline written in Python to SQL statements without requiring the user to rewrite any of them, as is required for existing tools such as Grizzly or pandas-to-sql3. Listing 6 shows the code to inspect the attributes race and age_group from an input pipeline stored as Listing3.py. The first part (lines 1-4) originates from the mlinspect framework and prepares the inspection steps. The second part (lines 5-7) executes the pipeline including inspection within a database system.

3.4.1 Choice: View/CTE. The users are able to choose if the whole pipeline is held in a CTE or views should be used (line 7: mode="CTE"/"VIEW"). In PostgreSQL, CTEs represent an optimisation barrier, which reduces the performance4. When choosing CTE as the target, the previous SQL operations must be included within the with clause for each query, for example, once for each inspected attribute. Whereas when creating a view for each query, less SQL code has to be generated. Nevertheless, each non-materialised view runs each query on demand.

3.4.2 Materialising a View/CTE. To avoid rerunning every query on demand, the user is also able to decide if intermediate views are materialised (line 7: materialize=True/False). Materialisation is interesting for views/CTEs that are expensive to calculate, contain few tuples and are used frequently. For example, if a query accesses a view at least twice, the accessed view is a candidate for materialisation. This applies to all fitting parameters that are calculated for the application of scikit-learn preprocessing functions (see Section 5.2). Materialising the number of occurrences per group also accelerates the runtime for inspections when comparing the ratios before and after some operations. Materialising a view or a CTE before the first operation is generally faster, as subsequent operations depend on its result. When the user chooses to materialise, all created views/CTEs, for which recalculating can be avoided, as well as all fitting parameters are materialised. On the other hand, when the database system provides main-memory capabilities, storing big intermediate tables might not be wanted as rerunning the query with the additional step performs as well as materialisation.

The decision to materialise a view/CTE is made after translating the Python code. Our implementation allows choosing between views and CTEs and whether to materialise them. The class SQLQueryContainer holds all SQL queries in a list. This also allows representing an SQL query as a CTE or as a view and to materialise it when needed.

Listing 6: Addressing the SQL target with inspection.

```python
inspector_result = PipelineInspector()
.on_pipeline_from_file("Listing3.py")
.add_custom_monkey_patching_module(custom_monkeypatching)
.on_pipeline_from_string(code)
.inspect()
```

Listing 7: Simple pipeline with inspection call.

```python
from mlinspect.instrumentation._pipeline_executor import 
set_code_reference_call, 
set_code_reference_subscript, 
monkey_patch, undo_monkey_patch

import pandas as pd
patients = pd.read_csv('path/to/p.csv', na_values='?')

histories = pd.read_csv('path/to/h.csv', na_values='?')
data = patients.merge(histories, on=['ssn'])
data["new_col"] = patients['children'] > 2

inspector_result = PipelineInspector()
.on_pipeline_from_string(code)
.add_check(NoBiasIntroducedFor('race'))
.execute()
```

4 TRANSPILING CODE

The mlinspect project is an extendable tool for lightweight inspection of data-preprocessing pipelines written in Python [8]. Support for additional Python libraries for data preprocessing can be added through backends and monkey-patching modules. Monkey-patching is a concept based on Python’s ability to extend its functionality of objects and functions at runtime5. Instead of modifying the user code, monkey-patching catches relevant function calls by their type and delegates the call to an alternative modified function. This approach considers functions only that are needed to support the inspection functionality. Additionally, nested calls are automatically executed in Python’s default execution order. Currently, only data pipelines created with pandas5 and scikit-learn [22] can be inspected. Scikit-learn and pandas are popular and constantly evolving libraries, so support for new functionality needs to be added over time.

Running mlinspect returns a datadflow directed acyclic graph (DAG) representing the pipeline and two dictionaries. One dictionary maps each check to its result and a second dictionary maps each DAG node to the inspection results associated with it. The dictionaries can be examined to see the checks that failed and the ones that passed.

The class PipelineInspector (Listing 7) initialises the setup in order to annotate the original source (code) for monkey-patching (Listing 8). Before execution, monkey-patching either adds the checks and inspections or replaces the whole function call as needed for an SQL backend. To deduce the table schema from the original Python code, the SQL backend runs the pipeline with a subset of the original data (e.g. ten rows) first. The main piece

3https://github.com/AmirPupko/pandas-to-sql
4https://www.postgresql.org/docs/12/queries-with.html
5https://pandas.pydata.org/docs/index.html
of the transpilation is the SQL mapping that maps each object the original Python source code creates, called dummy object, to the deduced information to create the corresponding representation in SQL (table expression). The SQL mapping is a hash-table with the Python dummy object as key and the deduced information as the value. The dummy object is either of the pandas.Series or DataFrame type. This is better suited as a key than a variable name as multiple dummy objects share the same name in the Python source code. To ensure that each name of a view or a CTE is unique, we assign a sequential number to its name in SQL. As each line of the source code might depend on previous operations, each table expression might also depend on previous ones. Each patched function is performed once on the Python object to deduce the table expression in SQL. In this way, the next operation working on the output knows which table expression to access. Before execution, the SQLQueryContainer generates all table expressions and the class SQLLogic embeds them in a view/CTE. The SQL mapping contains, in addition, the following information to allow combining queries and tracking tuples:

1. The Python dummy object.
2. List of tuple identifiers (index columns) currently associated with the Python dummy object.
3. List of non-index columns.
4. Execution tree of operations that lead to the current dummy object (used to resolve joins on the same table).

The list of identifiers contains the tuple identifiers that are needed to reconstruct a sensitive column during inspection. Each identifier has a unique name (<view/CTE-name> + _ctid), which is propagated throughout all operations. In our implementation, a dictionary in SQLHistogramForColumns maps the original column name in pandas to the table and the tuple identifier in SQL. When the mlinspect framework needs to inspect a sensitive column, it delegates the call to our SQL backend. The backend looks up the identifier in the dictionary to generate and execute the table expression that calculates the ratios and restores the column when needed.

Each patched function returns exactly what the original would return. This guarantees that the inspection does not distort any results. The modifications are entirely generic and, hence, are independent of the already presented implementation of the mlinspect’s backend and monkey-patching modules.

5.1.3 Selection and Projection. The selection and projection are subsumed together, as in pandas they are both accessed through the same function: __getitem__. Depending on the arguments, this function performs either operation.

If the argument is a string or a list of strings, a projection is meant where the strings name the columns.

With selections, the argument will frequently be a nested operation representing the selection condition. The only restriction is that the input evaluates to a pandas.Series of type bool, the criterion for keeping or removing rows. The pandas.Series is a single column of the pandas.DataFrame. As the operations are translated line by line, it is not known beforehand whether an operation is part of the result as a column or used within a selection condition. Internally, the SQL mapping maintains an execution tree. Each caught functions extends the execution tree. After processing all operations, the complete execution tree gets traversed to create the current table expression.

5.1.4 Arithmetic/Boolean Operations (e.g., +, *, >, &not). Applying monkey-patching to Listing 9 results in multiple single calls and cannot be translated into a single SQL query:

1. The projection data[’b’] returns a new pandas object, called pandas.Series(data_b)
2. The projection data[’c’] again leads to a new pandas object: pandas.Series(data_c)
3. Also the multiplication __rmul__(+) with the arguments 1.2 and pandas.Series(data_c) returns the new object pandas.Series(data_c_mul)
4. The comparison __gt__(>) operation with the arguments pandas.Series(data_b), pandas.Series(data_c_mul) returns pandas.Series(data_b_gt_data_c_mul)

5.1.5 Read from CSV. To load data from a CSV file to SQL, the file first needs to be created. This is done by analysing the CSV file and deriving the data types based on the content. Besides integers and floats, other types—objects in pandas—are considered as a string. Afterwards, the data is loaded using the COPY command in SQL. For tuple-tracking, a column with an identifier has to be added. In PostgreSQL, this is achieved by exposing the ctid.

Some pandas operations rely on a row number, for example, row-wise multiplications of two columns of different tables (see Section 5.1.8). For these operations, it is necessary to add the column to the original data structure. When working on a CSV file, for example, a new column could be added to the file before reading and storing the content in the database system. Actually, in two of the three example datasets in mlinspect, such columns are already present, so detection capability for such cases was added as well. The new table with the added columns will be used as the source in the SQL mapping.
A lookup table helps to translate the aggregation functions, which in pandas are named differently to those in SQL. It is necessary to rename or reimplement some custom functions from pandas before using them in SQL. For example, the pandas function std results in stdev_pop for SQL, mean in avg.

To enable inspection of aggregated values, their corresponding identifiers also have to be aggregated to an array using array_agg as part of the SQL query.

5.1.6 Drop Null Values. pandas’ dropna function allows any row containing null values to be dropped (see Figure 5). In SQL, a simple selection suffices. The selection condition consists of concatenated and negated is null blocks.

5.1.7 Replace. replace substitutes any value contained in a pandas object with another. By default, only whole strings are changed, but replacements by a regular expression are also possible. The SQL function REGEXP_REPLACE fits as a general solution, as alternatives like SQL’s REPLACE function replaces each instance of a word in an entry with a new one. To force the replacement of whole strings, the regular expression special characters ‘\’ and $ match the beginning of the string as well as the end (Listing 12).

5.1.8 Row-Wise Operations. The term row-wise refers to operations, where the n-th line of one table is combined with the n-th line of another table. By default, any pandas table contains an index column, but it is not semantically part of the table. Porting tb1 and tb2 to SQL causes no problem (Listing 13), although row-wise operations on columns of different source tables require an index column. We support the combination of two tables by the row number to mimic pandas functionality. The relational model is set-oriented, whereas pandas implicitly joins two tables with the same number of rows by the row number. The tuple identifier cannot be used to index the row number. Therefore, the function that creates a table, e.g. add_csv, also adds an index column if required (add_mlinspect_serial=True). It represents the row number needed for row-wise operations in SQL (Listing 14).

5.1.5 Group-By and Aggregation. A group-by with an additional aggregation consists of two parts in pandas (Listing 4 lines 28f). First, the group-by function is called on the pandas table, with the columns to group by as the argument. This function returns a specific group-by object, which is only needed when an additional aggregation is called. To translate the call, the columns to group by are stored until the aggregation functions is called.
5.2 Supported Scikit-Learn Functions

For many transformations in a preprocessing pipeline, specific parameters are calculated before the first use. For example, the SimpleImputer from scikit-learn (numbers 16 and 21 in Figure 1) calculates the replacement for null values before substitution [9]. The fitting step of a pipeline calculates these prerequisites for certain steps. The fitting needs to occur before transforming the passed data (see Figure 6). Furthermore, calculating the fitting parameters can be performed independently of transforming the data. If fitting was performed each time a transformation applied, the results would not be consistent. For example, the substitution for null values could be different for the training and the test set. This means that certain values need to be calculated exactly once and be accessible in the query from then on. These values should be materialised or cached, so that they do not need to be recalculated in each step.

### 5.2.1 Simple Imputer

The Simple imputer—as implemented in scikit-learn—replaces all null values in a table based on some metric, for example, most frequent, constant, mean and median. The SQL query to realise an impute consists of a nested subquery that aggregates the values according to a metric for the substitute and returns a single value to replace null values (Listing 15). For the case most frequent, the value that appears the most frequently is the substitute. The SQL function COALESCE assigns the first non-null value. As the values for substitution are calculated in the fitting step and are reused in each transformation step, their table expression is a candidate for materialisation.

```sql
WITH counts_help AS (  
    SELECT "label", COUNT(*) AS count FROM origin GROUP BY "label"  
  ), substitute AS (  
    SELECT "label" AS most_frequent FROM counts_help  
    WHERE counts_help.count = (SELECT MAX(count) FROM counts_help)  
    LIMIT 1  
  )  
SELECT COALESCE("label", (SELECT * FROM substitute)) AS "label" FROM origin
```

Listing 15: Simple imputer in SQL.

### 5.2.2 One-Hot-Encoder

One-hot-encoding transforms categorical data into a binary vector. The idea is to create an array with its size equal to the number of categories out of zero values besides a single one at the position of the current category.

The function `array_fill` creates an array filled with a constant value of a length passed through a second parameter. So one-hot-encoding can be implemented by taking the number `n`, which represents the number of categories (e.g., by counting distinct entries or with `RANK`), and creating an array with `n - 1` zeroes followed by a one and `n` zeroes once again. After creating such a representation for each sensitive column, a join brings all the values together to the final table (Listing 16).

```sql
WITH original_label_onehot AS (  
    SELECT "label", ARRAY[cast((SELECT count(DISTINCT("label"))) FROM original) AS int] AS "rank",  
    ) AS one_hot  
FROM (  
    SELECT "label", RANK_NUMBER() OVER () AS int FROM one_hot  
) AS count  
WHERE original."label" = original_label_onehot."label"
```

Listing 16: One-hot-encoding in SQL.

### 5.2.3 Standard Scaler

The standard score of a sample $x \in X$ is calculated as $z(l) = \frac{l - \text{mean}(x \in X)}{\text{stddev}(x \in X)}$. The mean and standard deviation is calculated in the fitting step (Listing 17) and reused for any other transformation.

```sql
SELECT ("label" - (SELECT AVG("label") FROM origin))  
/ (SELECT STDDEV_POP("label") FROM origin) AS "label" FROM origin
```

Listing 17: Standard scaler in SQL.

### 5.2.4 KBins Discretizer

The KBins discretizer from scikit-learn creates $k$ intervals or bins based on the training data in the fitting step. It then assigns each input value to a specific bin and returns an encoding representing the assigned bin. The first step is to calculate the step size $\text{step size} = \frac{\text{max}(x \in X) - \text{min}(x \in X)}{k - 1}$.

All values smaller than $\text{min}(x \in X) + \text{step size}$ are assigned to the first bin, which usually is 0. All values $l$ where $\text{min}(x \in X) + \text{step size} \leq l < \text{min}(x \in X) + 2 \cdot \text{step size}$ hold belong to the second bin and similarly for greater values.

So the bin is calculated as

$$
\text{bin}(l) = \left\lfloor \frac{l - \text{min}(x \in X)}{\text{step size}} \right\rfloor.
$$

Values smaller than $\text{min}(x \in X)$ and bigger than $\text{max}(x \in X)$ are possible, because the training data does not necessarily provide values smaller and bigger than the testing set, hence the edge cases are handled with the help of `LEAST` and `GREATEST` (Listing 18). Different strategies for calculating the bins exist, currently only the explained strategy called uniform is implemented.

```sql
SELECT LEAST(\text{GREATEST}(\text{FLOOR}("label" - (SELECT MIN("label") AS min_val FROM origin)) / (SELECT MAX("label") FROM origin) - (SELECT MIN("label") FROM origin) / 4 AS step)),  
AS "label" FROM origin
```

Listing 18: KBins discretizer in SQL (4 bins).

### 5.2.5 Binarize

Binarize decodes a value as one when surpassing a threshold or as zero otherwise, which is translated into a case statement in SQL (Listing 19).

```sql
SELECT CASE WHEN ("label" > 50) THEN 1 ELSE 0 END AS "label" FROM origin
```

Listing 19: Binarize in SQL (threshold 50).

---

Table 1: Pipelines with pandas and scikit-learn operations.

<table>
<thead>
<tr>
<th>healthcare</th>
<th>compas</th>
<th>adult simple</th>
<th>adult complex</th>
</tr>
</thead>
<tbody>
<tr>
<td>read_csv</td>
<td>read_csv</td>
<td>read_csv</td>
<td>read_csv</td>
</tr>
<tr>
<td>merge</td>
<td>miscellaneous operations</td>
<td>replace</td>
<td>label_binarize</td>
</tr>
<tr>
<td>groupby</td>
<td>label_binarize</td>
<td>SimpleImputer</td>
<td>SimpleImputer</td>
</tr>
<tr>
<td>add</td>
<td>StandardScaler</td>
<td>OneHotEncoder</td>
<td>OneHotEncoder</td>
</tr>
</tbody>
</table>

Table 2: Datasets used.

<table>
<thead>
<tr>
<th>healthcare patients.csv</th>
<th>compas_train.csv</th>
<th>adult_test.csv</th>
<th>adult_train.csv</th>
</tr>
</thead>
<tbody>
<tr>
<td>[smoker, complications, age_group]</td>
<td>[v_score_text, v_screening_date, in_custody, priors_count, start, end, event]</td>
<td>[c_charge_degree, c_charge_desc, type_of_assessment, v_charge_degree, v_charge_desc, v_decile_score, v_charge_degree.1, score_text, screening_date, in_custody, priors_count, start, end, event]</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Transpilation time to SQL.

<table>
<thead>
<tr>
<th>Category</th>
<th>VIEW</th>
<th>CTE</th>
<th>+ scikit-learn</th>
<th>VIEW</th>
<th>CTE</th>
<th>+ inspection</th>
<th>VIEW</th>
<th>CTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>healthcare</td>
<td>0.0585s</td>
<td>0.0505s</td>
<td>0.072s</td>
<td>0.0745s</td>
<td>0.1345s</td>
<td>0.079s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>compas</td>
<td>0.0765s</td>
<td>0.0805s</td>
<td>0.114s</td>
<td>0.113s</td>
<td>0.114s</td>
<td>0.120s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>adult simple</td>
<td>0.017s</td>
<td>0.018s</td>
<td>0.037s</td>
<td>0.035s</td>
<td>0.036s</td>
<td>0.035s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>adult complex</td>
<td>0.029s</td>
<td>0.031s</td>
<td>0.049s</td>
<td>0.047s</td>
<td>0.062s</td>
<td>0.050s</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6 EVALUATION

By extending the mlinspect framework by code-generation to SQL, we provide full support for executing pipelines within mlinspect while off-loading compute-intensive tasks to the database system. To measure the performance increase through the use of a database system, we compare the performance of selected pipelines using existing library functions to either common table expressions (CTEs) or materialised views. The pipelines are taken from the mlinspect repository and their names were not changed. The healthcare and compas pipelines work on the healthcare and compas dataset respectively. The pipelines called adult simple and adult complex both work on the adult dataset. Table 1 shows all the considered pipelines with the operations from pandas and the one from scikit-learn marked in grey. The benchmarks in Section 6.1 evaluate only the pandas operations and their SQL counterparts, whereas Section 6.2 also includes the scikit-learn operations and their translations into SQL. Section 6.3 presents the additional overhead when enabling inspection to detect technical biases. Finally, Section 6.4 shows the runtime of the original pipeline including training a neural network in Keras but with data preprocessing and inspection outsourced to a database system. Section 6.5 breaks down the runtime by the performed operations. Section 6.6 measures the impact of the number of sensitive columns on the runtime using the New York Taxi dataset. The depicted runtimes enclose a call to the psycopg2 adapter to run the query, so they include optimisation, compilation and execution time within the database systems. Transpilation to SQL took about 100ms for each pipeline (see Table 2), which we added to the measurements.

The original pipelines were either extended with generated mocking data or by replicating the original one until the desired size is reached (see Table 2). The used approach depends on the pipeline that is inspected, as some operations (e.g. join) will lead to big subresults for just replicated data. The first column of the compas and adult dataset each contains the pandas row numbers without a header. The mlinspect authors considered this case intentionally, as pandas recognises and handles missing headers.

In the following subsections, the performance differences are presented for all example pipelines in the mlinspect project repository. This is possible as transpilation to SQL including inspection is available without requiring any changes to the target pipeline.

System: Ubuntu 20.04.2 LTS, four cores of Intel i7-7700HQ CPU, running at 2.80 GHz clock frequency each, and 16 GiB RAM.
Software: PostgreSQL 12.7, Umbra, Python 3.8.10, Pandas 1.3.0

6.1 Pandas-to-SQL Performance

We first compare the performance of the operations in pandas only to the SQL translations. For each pipeline, all code up to the last line containing pandas code was translated to SQL and benchmarked against the original pipeline code up to the same line (see Figure 7a). For the comparison with pandas code, no view/CTE in SQL needs to be materialised, as all parts of the query are only executed once. The pipelines adult simple and adult complex have a negligibly small pandas part, which loads the data only.

We first discuss the performance of the pandas operations and their SQL translations for the healthcare pipeline. Umbra outperforms the operations in pandas by up to a factor of ten using CTEs and unmaterialised views (VIEW). PostgreSQL outperforms pandas with CTEs, but is able to outperform pandas with larger datasets using views by about a factor of two. It is interesting that the performance using CTEs differs from that using views within PostgreSQL. The reason is that the query for CTE did not contain any NOT MATERIALIZED statements to avoid materialising the intermediate CTEs. All CTEs—materialised or not—are accessed only once resulting in the inefficiency of materialising unnecessary data. If NOT MATERIALIZED was added to all CTEs, the performance would be closer to the VIEW one.

The second benchmark is based on the compas pipeline. This pipeline differs from the first one, which splits one dataset into train and test sets, as it uses two different datasets for training and testing. The way the SQL translation is implemented, only the parts contributing to the result of the pipeline are executed, or alternatively the most recent call. Code not contributing to the pipeline, like prints or operations on unused tables, are skipped. For a fair comparison, we only execute the part of the compas pipeline handling the training data. The excluded lines would load the unused test set and apply a simple projection. Umbra outperformed pandas by up to a factor of five. PostgreSQL outperforms pandas as well but by a lesser margin than Umbra.

These results show that a modern database systems as Umbra performs data preprocessing faster than using dataframes in pandas. With unmaterialised views, PostgreSQL preprocess data faster than pandas dataframes.
Figure 7: Runtime results for a) the operations in pandas, b) plus the operations in scikit-learn and c) plus inspection.
6.2 Pandas/Scikit-Learn-to-SQL Performance

In practise, it will be highly unlikely to find a pipeline just made of pandas operations [54]. This subsection evaluates the performance of the entire preprocessing pipeline but without training or inspection. This additionally includes operations from the scikit-learn library. Scikit-learn calculates the fitting parameters, which subsequent steps in the pipeline access afterwards. As monkey-patching rewrites each individual function call, this generates one table expression for each fitting parameter although each parameter is based on the same tuples. So materialising the table expressions needed for the fitting parameters accelerates the PostgreSQL runs with VIEW as this avoids redundant executions.

PostgreSQL outperforms pandas in most of the runs (see Figure 7b). For the healthcare pipeline, Umbra outperformed the original one by up to a factor of 150 and even the run in PostgreSQL with materialised views by up to a factor of 10. The performance gain with Umbra for $10^6$ tuples varied between a factor of 40 (adult simple) and $5 \cdot 10^3$ (adult complex). Since the measurements include the transpilation time to generate the SQL queries, the plots indicate that the additional overhead is amortised from at least $10^4$ tuples. To conclude, database systems show their full potential when preprocessing large datasets. Next, we will show how inspection influences the runtime.

6.3 Inspection Performance

This subsection discusses the performance when data inspection for the pipelines is enabled. Here, the materialisation of intermediate results becomes even more important as the inspection is applied after each operation. $n$ inspection steps lead to $n$ executions of the first operation, $n - 1$ executions of the second operation and so on.

With an increasing number of tuples, all database systems execute the additional inspection steps faster (see Figure 7c). For $10^8$ tuples, PostgreSQL outperformed the original inspection run with pandas/scikit-learn by between a factor of five (compas) and almost $100$ (adult complex). Umbra accelerated inspection on the same datasets by a factor of 2 (compas) and $200$ (adult complex) compared to the original run. To summarise, our approach with SQL queries accelerates inspection of pipelines out of pandas and scikit-learn operations on datasets of size $10^n$ onwards.

6.4 End-to-End Performance Comparison

To show that this approach can substitute whole end-to-end preprocessing pipelines and integrates well with training, this subsection benchmarks the whole pipeline with the original datasets of mlinspect (9771 tuples for the adult, 889 tuples for the healthcare and 2167 tuples for the compas dataset). This will show the advanced state of the implementation and its potential when transferring and transforming data as investigated in the next subsection in more detail. Both pipelines on the adult dataset predict the income (less or greater than/equal to $50k$), the healthcare pipeline computes a score as the probability of complications and the compas pipeline uses logistic regression to predict a score (high/low). The correctness is verified by comparing the equality of the intermediate results (see Figure 9, Table 4). The accuracies of the trained model for the healthcare and the adult complex pipeline differ slightly because of the stochastic nature of the train/test split and the training (see Table 5).

For the presented end-to-end runs, the adult and the compas datasets are large enough that the corresponding pipelines benefit...
from accelerated preprocessing (see Figure 8). For the healthcare pipeline, PostgreSQL and the default pipeline seem to perform about the same. The reason is that the training time for the model is significantly higher here, which results in a smaller impact from the accelerated preprocessing. Processing within the database systems requires extraction, the transforming and loading of data for subsequent model training. The transformation consists of a cast into a matrix representation (NumPy array) to feed the model. This step will be skipped if the data already lies with the database system and the training happens there as well, as proposed for Umbra and HyPer [33, 34, 41, 46, 47].

6.5 Operation Level Performance

System (this experiment only): Ubuntu 20.04.2 LTS, AMD Ryzen 7 4800H, 8 cores (16 threads), 2.9 GHz, 32 GB of DDR4 RAM (3200 MHz), 512 GB of SSD (1x M.2 2280 SSD via PCI Express 3.0 x4).

To investigate how and where the speedups come from, Figure 10 shows the compas pipeline broken down into each operation. The two plots show the pipeline with replicated data for two different input sizes ($10^6$/10$^7$ tuples).

When inspecting the runtimes for the different pipelines, most operations are performed faster in PostgreSQL than in Python. The binarize operations took about 10 ms for PostgreSQL (a simple case statement in SQL) and therefore are hardly visible within the plots. The scoring step to calculate the accuracy accesses all tuples and is therefore time-consuming within a disk-based database system. The time PostgreSQL loses due to additional data loading and extraction could be eliminated when all computations happen inside database systems.

Overall, a significant increase in performance was achieved throughout all pipelines. This is especially promising as the examples were not artificially constructed or simplified. Instead, realistic pipelines were tested. The price for data loading and transformation is a worthwhile one compared to the other performance gains. The performance of Umbra paired with the additional benefits of training the models in the database system appears to be a promising approach worth pursuing.

6.6 Varying the Number of Columns

To measure the impact of the number of inspected columns on the runtime, we vary the number of sensitive columns. We use one month—January 2019 (7,667,793 tuples) and January 2021 (cleaned: 1,271,414 tuples)—of the New York Taxi dataset, where we perform one operation (selection: passenger_count > 1) only. We initially inspect the column passenger_count only and expand the inspection stepwise to encompass the following columns: trip_distance, PULocationID, DOLocationID and payment_type. Figure 11 shows the runtime depending on the number of inspected columns. All database systems execute the inspections faster than pandas. In PostgreSQL, the runtime of the CTE version increases linearly with the number of inspected columns, which is expected as the whole query runs once for each column. Nevertheless, the view version performs better as views are part of the holistic query optimisation in PostgreSQL. In Umbra, both versions show similar performance.

7 CONCLUSION

This paper has presented SQL queries for bias detection caused by data preprocessing. By exposing the tuple identifier throughout all operations, we were able to track the distribution frequency within columns that were even removed during preprocessing. In order to automatically generate these queries, we extended the mlinspect framework with a backend that replaces calls to Python library functions with SQL queries using monkey-patching. Our backend translated each line of the original Python source code into one CTE/view. One CTE or view per sensitive column calculated the ratios needed to detect introduced biases. Our evaluation revealed that materialised views in PostgreSQL could improve the overall preprocessing and inspection performance for larger datasets. The performance could be further improved using Umbra with in-memory performance even without the need to materialise intermediate results. An extension to support further library functions such as for training a model would eliminate the remaining need for final data transfer and thus further improve the performance.

1https://www1.nyc.gov/site/tlc/about/tlc-trip-record-data.page