Outline:

Abstract: describe four main points of this method.

Introduction: Describe the context: spaghetti environments. Describe key terminology.

Previous Work: SUBDUE, GBAD, Genga.

Approach: Algorithmic details

Evaluation:

Conclusions and Future Work

Definition of noise: A high variance branch between several optional activities

Definition of anomaly: An event which occurs in the context of a normative pattern.

Abstract

This paper discusses an unsupervised, threshold-based method for anomaly detection and normative-pattern mining using the iterative SUBDUE graph compression method and the Inductive Miner. We provide an overview of process mining definitions and existing approaches, then test the method on synthetic data provided by a data generation algorithm. This approach requires a single parameter describing the anomaly threshold. In turn, the method generates a dendrogram, a taxonomical representation of compressing activity features by which further automated or human analysis may be performed. This method provides a framework by which many organizational, technological, and natural processes can be monitored and modeled.

Introduction

As described in [VDA], a Process Aware Information System is defined as *a software system that manages and executes operational processes involving people, applications, and/or information sources on the basis of process models [VDA].* This formal definition simply distinguishes operational management systems as systems which are both aware of process data and likewise prescribe tasks and activities per prescribed process models. Thus, such systems incorporate process data and process models in a feedback loop whereby processes can be tracked, defined, and organized via process models; likewise, process models may be derived and analyzed based on process data.

In real-world scenarios, many enterprises rely on many overlapping but non-interoperable systems, enterprise management systems, and tribal knowledge to monitor and control processes, such that the overarching requirements of formal PAIS’s become infeasible or intrusive. This paper focuses on contexts for which a PAIS is instead an abstraction consuming noisy process data derived from multiple systems, and from which process models can be mined and analyzed to improve processes. This interpretation is more amenable to less process-prescriptive scenarios in which activities execute within an embedded framework of changing people, tools, resources, and institutional knowledge. In this scenario, a PAIS is a collection of operational systems and disparate data sources by which one derives traces characterizing the underlying process-oriented view of institutional activities.

In this context, the ability to mine and analyze normative process patterns is critical for extracting actionable information and detecting unusual activity. Detection requires some prior normative activity patterns by which to detect anomalous behavior, hence these are complementary tasks. To this end, we present a method for mining process patterns from workflow logs that also exhibits useful anomaly detection properties, using the Inductive Miner to construct a graphical process model, then applying the SUBDUE graph compression method to iteratively extract the normative patterns of this model. Lastly, anomalies and other useful features may be found in post-processing.

This hybrid approach is useful since the Inductive Miner extracts generality from process log data, outputting a graphical model *M* capable of generating all traces in a process log, regardless of how overly-inclusive or how noisy the input log. SUBDUE then constructs a hierarchy of structures of *M* most relevant to the log as a dendrogram, effectively extracting from M its most informative components. In short, for a given trace log, the Inductive Miner is used to mine the most general process model, then SUBDUE is used to extract only the most specific components of the model. Using this unsupervised method, one can mine normative process patterns, detect anomalies to those patterns, and perform other analyses.

The preceding captures the spirit and contribution of our method, but some definitions are needed. From the control-flow perspective, common process mining terms can be framed in a familiar graph-theoretic manner:

-process model: In this work, a graph with vertices representing activities, and edges representing transitions between activities. Processes can contain many constructs representing linear and non-linear constructs, and a variety of notations and languages have been defined over the space of process models. The notable example is the Petri-Net [CITE].

-process grammar: Constructs defining common process traversal patterns. For example, an AND-SPLIT is a set of edges branching from a single node and traversing activities in parallel before synchronizing at some later activity. Other constructs include OR-SPLIT, XOR, LOOP, JOIN, and so on.

-workflow trace: A single execution of a process as a partially-ordered sequence of activities, which is any valid path from some START node to an END node on the process model. This is best represented as a string composed of letters representing the activities traversed.

-workflow log: A set of workflow traces, for which various measures are taken to mitigate properties such as noise or incompleteness.

-process miner: An algorithm for constructing a process model from a workflow log, per criteria such as specificity and generality. Specificity favors restrictive models including only (or less than) the behavior described by the workflow log, whereas generality favors larger models describing all traces and potentially additional behavior.

-partial-order property: The property by which activities within a workflow trace may be randomly ordered with respect to parallel activities. ‘ABCD’ and ‘ACBD’ might be workflow traces from some model, where ‘C’ and ‘B’ are parallel sub-processes, and may themselves recursively embody further parallel sub-processes, and ‘A’ always occurs before ‘D’. The explosive number of possible models defined over a log of partially-ordered traces represents a primary challenge for process mining algorithms, whose task is disambiguating the partial order property by applying various rules and heuristics per pre-defined criteria of specificity and generality to output models with desired properties.

-spaghetti model: A workflow defined by highly diverse, informal, and possibly disorderly behavior, typically containing many scattered, repetitive events. These represent immature business processes, in contrast to “lasagna” processes with structured, stratified behavioral logic.

-inductive miner: The process mining algorithm that, given a workflow log, generates a graphical process model capturing the most general, all-inclusive view of the traces. For our purposes, this model is used in pre-processing to convert a workflow log of partially-ordered traces into a collection of subgraphs.

-SUBDUE: Short for “Substructure Discovery”, this method searches over a collection of graphs and, by applying the minimum-description-length principle, returns the top-k most compressing sub-graphs [CITE].

-GBAD: Short for “graph-based anomaly detection”, this method internally calls SUBDUE, then implements methods for detecting anomalies occurring in the context of discovered patterns.

A more in-depth overview of process mining terms and methods can be found in [VDA book].

Previous Work

The SUBDUE graph-compression method accommodates any context of mining graph data for normative patterns, and hence works as a graph-based feature detector. It was previously used for knowledge representation systems [CITE EARLIEST], and more recently in security applications for intrusion detection [NOBLE]. Using SUBDUE as a process mining tool has been successfully performed by [GENGA et al], whose results demonstrated the method’s utility for “spaghetti processes” describing more realistic institutional processes.

GBAD has also been deployed to detect anomalous activities, particularly within the immediate proximity of discovered normative patterns. This is appropriate for safety-critical and security contexts for which there exists some underlying, prescribed process model by which normative patterns can be assumed to have a ground-truth policy, but less so when the underlying process is not prescribed.

Previous work on process anomaly detection focuses primarily on the mining process itself and on trace-scoring schemes. [VDA] details scoring schemes, by which work traces are replayed on a discovered model, assigned a numeric fitness score, and the anomalies determined based on a discriminative threshold. Bezerra’s work examined anomaly detection using several threshold-based approaches within the process mining algorithm itself [CITE]. Bezerra decomposed this family of process-based anomaly detection into three groups: threshold-based, iterative, and sampling. Although closely related, our approach does not fit into these methods since it is compression based: a generic process model is mined, graphical features detected, and anomalies are detected and reported in post-processing. Our work replicates Bezerra’s data generation methods, but otherwise builds on this work by applying anomaly detection in post-processing of discovered process models.

The Method

Under our relaxed definition, a PAIS is a composition of process monitoring systems from which workflow traces can be extracted for process mining. We assume such transformation steps have completed, and process data converted into a popular log format such as Extensible Event Stream (XES). Our method decomposes to three tasks: mine the generalized process model describing the workflow log, extract the log’s most descriptive normative graphical patterns, and finally detect outliers and anomalies with respect to these learned patterns.

For the first task, the Inductive Miner was suitable for mining the most general, graphical process model described by some log. This model is typically overly-inclusive, hence the second and third tasks discover the patterns and features most relevant to describe the log. For this task, we use the SUBDUE graph-compression method to discover the normative patterns, which in turn allows one to detect anomalies.

[visual]

The workflow of these tasks extends to any context in which one wishes to discover the overall characteristics of a process without respect to prior constraints, such as prescribed process models. Our approach extends to more realistic and informal “spaghetti” model scenarios in which processes are organically-defined to the point of being chaotic: enterprises, communication networks, fraudulent or criminal networks, and so on.

Using Graph Compression to Discover and Cluster Patterns

The SUBDUE [Holder] method discovers highly compressing patterns in graph data using the minimum description length (mdl) principle to discover and output the most compressing patterns. SUBDUE works by searching across the set of all subgraphs within a set of input graphs for the most highly-compressing patterns using the mdl principle.

This property of SUBDUE satisfies the requirement for an unsupervised method for discovering the most meaningful components of some graphical process model, since a workflow log is also a set of subgraphs generated by a process model. The Inductive Miner complements our approach, providing the super-graph process model by which the log traces can be converted from partially-ordered activities into subgraphs; these subgraphs are passed to SUBDUE to discover meaningful patterns.

Prior work on SUBDUE showed great potential when running the method iteratively on a set of graphs [NOBLE COOK]. At each iteration, the most compressing subgraph discovered by SUBDUE is used to replace all such instances with a single node, and then the method repeats until no further compression is possible. At the end, one obtains a recursive and hierarchical description of a set of graphs, in which the graph has been compressed away by recursively-defined subgraphs, all of which have been aliased and replaced by single nodes.

We tested a similar approach using GBAD, by which workflow traces were iteratively recompressed using the most-compressing subgraph found at each iteration. The three anomaly detection methods of GBAD were then used to detect anomalies at each iteration. While successful in terms of discovering patterns, this method suffered a high false positive rate for anomaly detection. Ultimately, the problem lies with iterative recompression: on successive iterations, the most highly compressing subgraph was often only a small alteration of node substitution, deletion, or insertion to a compressing subgraph found on a previous iteration. GBAD’s primary deficiency in this context is that its anomaly-detection methods apply to the local vicinity of the compressing pattern discovered by SUBDUE. Hence, the search space was highly redundant, often analyzing the same regions of the graph, but failing to reach the further reaches where compressing structure decays, and where anomalies often lie.

Since the requirement was to force SUBDUE to analyze new regions of the graphs, the remedy was to simply delete all instances of the most-compressing subgraph from the traces. The effect is that SUBDUE is encouraged to discover dissimilar graphical features, compressing away primary graphical features until only the least compressing features remain. As such, the method generates a natural, hierarchical derivation of process substructures in the form of a dendrogram. The dendrogram comprises the entire behavior of the log, with the most relevant and frequent graphical features located higher. This is amenable to anomaly detection since the less compressing a feature is, the more deviation it represents with respect to normative patterns and normal overall behavior, and hence will be placed lower in the dendrogram.

[visual]

This gives the following process-oriented pattern-mining algorithm:

[algo text]

As shown, the Inductive Miner takes a workflow log and returns a process model, by which the traces can be re-generated as a collection of subgraphs. This is fed to SUBDUE to find the most compressing substructure, which is appended to the dendrogram before being deleted from all traces in which it occurs. This step repeats until no further progress can be made and all traces have been compressed to their most elementary substructures. The dendrogram is returned, whose edges represent ancestry between compressing substructures and their constituent traces.

The success of this method lies in the dendrogram, as a descriptive model of the input log. The dendrogram can be analyzed in post-processing for common process features, redundant behavior, outliers, anomalies, and so on. [GENGA et al] have successfully detailed the uses for similar SUBDUE-based dendrograms, especially in the context of spaghetti processes cohering to no strict process definition.

This method belongs to the family of dendrogram or tree-induction methods in process mining literature [CITE SOME], and anomaly detection is just one use among many for querying the dendrogram. For instance, while the low-frequency, outlier components of the dendrogram may characterize anomalies and noise, the ancestral components encode the most relevant substructures of the workflow log. With this information, the process model returned by the Inductive Miner could be reduced to give a more concise process description. In this regard, coupling SUBDUE with the generalization feature of the Inductive Miner creates an extensible framework for more concise modelling of unstructured “spaghetti” process environments. Similarly, an analyst may examine highly similar components of the dendrogram, representing duplicate work or poor cohesion amongst business processes. Thus, the dendrogram extends to a range of pattern mining and other enterprise uses, beyond the scope of anomaly detection.

Anomaly detection lends an illustrative example in this context because of the structural characteristics of the dendrogram: given that anomalies are assumed to be infrequent events, subgraphs containing these will be among the last components compressed. The result is that for power-law distributed processes, the size of the dendrogram components decreases smoothly, then drops suddenly, such that the only remaining traces/subgraphs are those representing anomalies, outliers, or noise in the log.

Algorithm Evaluation

Although real process-oriented datasets are available, they do not offer the controlled conditions sufficient to compare the characteristics of different algorithms. We instead opted to use a synthetic data generation algorithm similar to [BEZERRA, Appendix A], which was modified slightly to generate data directly from probability distributions embedded in the generated models. This approach generates random process models from which synthetic traces are generated, and thus the performance of an anomaly detection method can be assessed with respect to a known model. Likewise, to cohere to a stable performance baseline, we also used the same experimental parameters as described in [BEZERRA]: 60 randomly-generated process models, 1000 traces.

Data Generation Algorithm

The data generation algorithm consisted of two steps: process model generation, and generating traces from these models. The first step was generating graphical process models, under a set of parameters describing the probability of generating various recursive structural features. These features include SEQ, OR-SPLIT, AND-SPLIT, and LOOP, defined as follows.

SEQ: the appending of a single activity.

OR-SPLIT: a single activity splits to one of two successors.

AND-SPLIT: a single activity splits to two parallel activities, both of which are traversed.

LOOP: An activity splits to a loop construct, then returns to that activity and continues.

These recursive operators generate directed, cyclic graphs of arbitrary complexity, given the constraint that the graph start at a START node and all paths eventually end at some END node. Additionally, since an “activity” is defined as a potentially null transition, the split constructs may divert to more than two activity paths, and so on. The parameters constrain model complexity to a probability distribution over these operators.

A second set of parameters defines the trace-generation distribution constraining the graphical walks of traces, which is only defined for OR-SPLIT and LOOP, since only these constructs contain choice behavior. To ensure maximum partial-order entropy, activities lying within the same timestep are shuffled such that they achieve uniform random behavior.

Lastly, since probabilistic model-generation allows for the possibility of unusual models, some basic tests are applied to ensure sufficient complexity. These include verifying the model contain a minimum START-END path length, maximum number of anomalies, maximum number anomalous edges within an anomaly (to constrain anomaly size), minimum number of unique activities, and minimum number of paths from START to END.

The models output by this method are thereby guaranteed to achieve sufficient complexity, and further that they generate an exponential distribution over unique traces.

Results

Conclusions and Future Work

The method presented here demonstrates the desirable qualities shared by any anomaly detection approach: strong normative pattern definitions, and strong separation between anomalies and normative patterns. This method has been shown to satisfy both requirements, strongly distinguishing anomalous traces, and generating normative patterns by which other process mining tasks can be performed. Notably, these properties satisfy a range of other process and monitoring tasks, as well as other process and graph mining tasks in fields such as biology, pharmacology, and chemical interaction.

The drawback to this method is its lack of noise-tolerance, a common problem faced by mining algorithms. While SUBDUE can find graphical patterns in an unsupervised manner, they become the only patterns by which the log is compressed further; that is, even small deviations to the normative pattern are ignored, and may be flagged as anomalies later. From an anomaly-detection perspective, this strongly discriminatory behavior is desirable. On the other hand, from a process mining perspective, the goal is often to mitigate such strong discrimination and to discover process models with a balanced, noise-tolerant tradeoff between specificity and generality. This yields the recurring discussion on specificity-generalization tradeoffs, to which all process mining approaches are subject. Future work lies in making the approach more noise tolerant, similar to how the GBAD system determines acceptable deviations in the local context of a normative pattern discovered by SUBDUE using graph distance metrics.

Ubiquitous computing populate enterprise databases with traces which, from the perspective of process mining, contain “process aware” data. Mining such data provides valuable insights into the structural characteristics of various process flows, and into the normative patterns by which anomalies can be detected in an unsupervised manner.

-describe traces, “process-aware” data, partial orderings, trace-logs

-describe use cases: structural analysis and anomaly detection. Benefit of our method is it is unsupervised.

-mention that discovered anomalies can be used to discover other anomalous instances in the log, results from doing so

-mention the overarching aim that the dendrogram characteristic is amenable to process-mining/anomaly detection in that well-defined process *ought to be* compressible; hence the well-defined, well-enforced process definitions yield better awareness of anomalies when they occur. Therefore the dendrogram “elbow” perspective is amenable to process mining, for which at least some underlying process structure can be estimated.

Definitions of Anomalies and Normative Patterns: focus on the “bump” in the dendrogram

Prior: Formulate goals of a process mining approach to anomaly detection, now describe how that maps onto the use of SUBDUE to accomplish these ends. Describe benefits of an algorithm used to derive partial-order mappings (process models) using the inductive miner.

Experiment

One of the primary difficulties in testing process mining strategies is a lack of stable experimental baselines for evaluating the properties of different methods, whether the methods are for process mining or anomaly detection (although the latter typically entails the former).

Definitions:

Anomaly: An anomaly is a trace that occurs in the context of a normative pattern.

Outlier: Outliers are defined as noise due to variance in some process’ execution. These are typically not strongly-associated with the underlying process model.

Refer to this work for graph anomaly definitions:

http://www3.cs.stonybrook.edu/~leman/pubs/14-dami-graphanomalysurvey.pdf

Related work:

Genga et al, multiple works using SUBDUE to generate process descriptions. Other trace analyzers and anomaly detection methods.

Conclusion