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