Robust Analysis of MAP Inference in Selective Sum-Product Networks

Julissa Villanueva Llerena
Denis Deratani Mauá

Department of Computer Science, Institute of Mathematics and Statistics, University of São Paulo, Brazil

Abstract

Sum-Product Networks (SPN) are deep probabilistic models that have shown to achieve state-of-the-art performance in several machine learning tasks. As with many other probabilistic models, performing Maximum-A-Posteriori (MAP) inference is NP-hard in SPNs. A notable exception is selective SPNs, that constrain the network so as to allow MAP inference to be performed in linear time. Due to the high number of parameters, SPNs learned from data can produce unreliable and overconfident inference; this phenomenon can be partially mitigated by performing a Robustness Analysis of the model predictions to changes in the parameters. In this work, we address the problem of assessing the robustness of MAP inferences produced with Selective SPNs to global perturbations of the parameters. We present efficient algorithms and an empirical analysis with realistic problems.

Keywords: Robust statistics, sensitivity analysis, sum-product networks, tractable probabilistic models.

1. Introduction

Sum-Product Networks (SPNs) are a class of deep probabilistic graphical models with an intuitive semantics given by context-specific independences [27, 23, 34, 14, 31]. An SPN represents a probability distribution over a set of random variables by a rooted directed-acyclic graph with tractable distributions as leaves, and weighted sums and product operations as inner nodes [27].

SPNs have obtained impressive results in many machine learning tasks due to their ability to represent complicated multidimensional distributions [27, 1, 37, 29, 28, 8, 26]. While SPNs allow for linear time predictive inference (i.e., computing the probability of a joint configuration of the variables), many tasks are more effectively solved by finding a maximal probability joint configuration of the variables that is consistent with a given evidence, a problem known as Maximum-A-Posteriori (MAP) inference [27, 35, 10]. This problem is known to be NP-hard even to approximate, and even for shallow structures [24, 10]. A notable exception is when SPNs are selective, that is, when the sub-networks of each sum node define distributions with disjoint supports. Selective SPNs admit MAP inference in linear time by a simple and parallelizable greedy algorithm [23, 24]. While selective SPNs are less expressive than non-selective SPNs [9, Theorem 4], empirical results have shown that learned selective SPNs obtain performance comparable to learned non-selective SPNS [23].

In spite of its relative success, and on par with other probabilistic models, SPNs learned from data generalize poorly on regions with insufficient statistical support, leading to unreliable, overconfident and prior-dependent conclusions. This issue can be mitigated by performing a sensitivity analysis of the model predictions to changes in the parameters [2]. Let us clarify the way we intend sensitivity analysis here, and in doing so, let us review related work.

Sensitivity analysis can be split into quantitative approaches and qualitative approaches. The former evaluate the effect of perturbation in the model parameters on the value of a particular inference. The latter concerns the classification of inferences into robust or not, depending on how an inference changes according to changes in the model parameters. Most of the previous work in sensitivity analysis in probabilistic graphical models is quantitative, with particular focus on the computation of marginal posterior probabilities over a single variable [15, 32, 20, 4, 6, 18, 16, 5]. Qualitative sensitivity analysis received much less attention, with some notable examples [21, 7, 30]. A second distinction can be made between local and global analyses. The former considers the effect of the perturbation of a single parameter, or a small group of related parameters; the latter aims at more general perturbations possibly affecting all the parameters of the model simultaneously. Initial work on algorithms for sensitivity analysis in probabilistic graphical models focused on local perturbations [5, 18]; more recently, algorithms for global analyses have been proposed [4, 6, 16].

The only approach to global sensitivity analysis in SPNs is the recent work by Mauá et al. [21], who considered Credal SPNs, that is, sets of SPNs obtained by a simultaneous perturbation of all model parameters. They developed efficient algorithms for producing upper and lower bound on the probability of evidence, and for performing credal classification for small number of classes. Importantly, they showed that performing global quantitative sensitivity analysis of MAP inference in these models is NP-hard.

In this work we develop efficient algorithms for global quantitative analysis of MAP inference in selective SPNs. In particular, we devise a polynomial-time procedure to decide whether a given MAP configuration is admissible.
We start with some notation and terminology. We write $w_S$ where $S$ is the root; and $x$ not consistent with $S$ is an indicator node consistent with $x; S(x) = 0$ if $S$ is an indicator node not consistent with $x; S(x) = \sum_{j \in ch(i)} w_{ij} S'(x)$, where $i$ is the root; and $S(x) = \prod_{j \in ch(i)} S'(x)$. This value can be computed in linear time by traversing the network from the leaves towards the root (caching values). For example, the evaluation of the SPN in Figure 1 at $X_0 = 1, X_1 = 1$ and $X_2 = 0$ is $S(x) = 0.4(1 \times 0.7 \times 0.4) + 0.6(0.2 \times 0.9 \times 0) = 0.112$.

In order to ensure that an SPN represents a valid distribution [27], we impose the following conditions:

- Completeness: The children of a sum node have identical scope;
- Decomposition: The children of a product node have disjoint scopes;
- Normalization: The sum of the weights of arcs leaving a sum node is one.

The SPN in Figure 1 is complete, decomposable, and normalized. For the rest of this paper, we assume that SPNs are complete, decomposable and normalized.

To ensure linear time MAP inference [23], we also impose the following additional property:

- Selectivity: At most one child sub-network of any sum node evaluates to nonzero at any realization of its scope.

The SPN in Figure 1 is selective. An alternative way to state the above condition is to assume that the supports of the distributions induced by the children of any sum node are disjoint. This implies for any realization $x$ and sum node $i$ that $S'(x) = w_{ij} S'(x)$ for $j \in ch(i)$.

Given a realization $x$ we say that a node $i$ of an SPN $S$ is active if $S'(x) > 0$. If the network is selective then at most one child of each sum node is active for any realization. The calculation tree $T_S$ of an SPN $S$ is the SPN induced by the sequence of active nodes for $x$ rooted at the root of $S$. Due to the decomposition property, the calculation tree of a selective SPN is a tree, hence justifying its name. In this case, we have that

$$T_S(x) = \prod_{i \rightarrow j \in T_S(x)} w_{ij}. \quad (1)$$

Figure 1: Selective Sum-Product Network over three binary variables.
In Figure 1, the sub-SPN induced by highlighted arcs represents the calculation tree for \( X_0 = X_1 = X_2 = 0 \), and \( T(0,0,0) = 0.6 \times 0.8 \times 0.9 = 0.432 \).

### 3.1. Learning Selective Sum-Product Networks

Given a dataset \( \mathcal{D} \) of i.i.d. realizations \( x \in \text{val}(X) \), Equation (1) allows us to obtain a closed-form maximum likelihood estimator for the weights of a fixed-structure selective SPN \( S \) by

\[
 w_{ij} = \frac{N_j}{N_i}, \tag{2}
\]

where \( N_k = |x \in \mathcal{D} : k \in T_k(x)| \) is the number of calculation trees containing node \( k \). We can obtain more robust estimators by smoothing the count above, for example, by using the estimator \( \hat{w}_{ij} = (N_j + s_j)/(N_j + s) \) for \( s = \sum_j s_j \). A common choice is Laplace smoothing, which uses \( s_j = 1 \). Note that this is equivalent to obtain Bayesian estimators assuming independent Dirichlet priors on the weights associated with a sum node.

Inspired by structure learning of standard probabilistic graphical models [17] and Equation (2), Peharz et al. [23] proposed learning selective SPNs by maximizing a penalized log-likelihood function that discounts the size of the graph of the data log-likelihood. They developed an algorithm that learn selective SPNs by performing a greedy hill-climbing search in the space of structures.

More recently, Liang et al. [19] developed an algorithm to learning Probabilistic Setential Decision Diagrams, a similar type of probabilistic models which can efficiently be translated into selective sum-product networks. At each step, their algorithm performs local modifications to the network that improve the test-set penalized log-likelihood. They show state-of-the-art performance according to test-set likelihood in benchmarks when learning ensemble of PSDDs using bagging and an EM-like procedure. Note however that the use of ensembles makes MAP inference NP-hard [10].

### 3.2. Maximum-A-Posteriori Inference

A normalized SPN \( S \) induces a probability measure \( P_S \) over the domain of its scope. Thus, given an SPN \( S \) with scope \( \{X, E\} \) and evidence \( e \in \text{val}(E) \), we define the set of MAP instantiations as:

\[
 x^* = \arg \max_{x \in \text{val}(X)} P(X|e) = \arg \max_{x \in \text{val}(X)} S(x, e).
\]

Although MAP inference is NP-hard in SPN even when restricted to binary variables and height-two networks [10, 33, 22, 25], the problem is solvable in linear time in the size of the network for Selective SPNs by the simple Max-Product algorithm [23, 25]. This algorithm consists in replacing sum operations with maximizations (obtaining a so-called Max-Product network), then evaluating the network by traversing nodes from the leaves towards the root. We say that a leaf node is consistent if its scope is in \( X \), or if its scope is \( E \) and the node evaluates to 1 at \( e \). The algorithm can be described by the following recursion (caching values to achieve linear time):

\[
 \text{MAP}^i = \begin{cases} 
 1 & \text{if } i \text{ is a consistent leaf node}, \\
 0 & \text{if } i \text{ is an inconsistent leaf}, \\
 \max_{j \in \text{child}(i)} \text{MAP}^j & \text{if } i \text{ is a product node}, \\
 \prod_{j \in \text{child}(i)} \text{MAP}^j & \text{if } i \text{ is a sum node}.
\end{cases}
\]

The corresponding MAP instantiation is obtained by backtracking the solutions of the maximizations from the root toward the leaves. The circuit tree in Figure 1 contains the arcs selected by Max-Product when backtracking from the root (i.e., it contains the arguments of the maximizations).

### 4. Credal Sum-Product Networks

We denote by \( S_w \) an SPN whose weights are \( w \). A Credal SPN (CSPN) is a set of (consistent, decomposable and normalized) SPNs \( \{S_w : w \in \mathcal{W}\} \) which all share the same network structure [21]. The space of weights \( \mathcal{W} \) is usually taken as the Cartesian product of closed and convex sets of weights \( \mathcal{W}_i \), one for each sum node \( i \) in the network. Since, the networks are normalized, a CSPN induces a credal set over the weights associated with outgoing edges of each sum node. An example of CSPN is shown in Figure 2.

Mauá et al. [21] developed a polynomial-time algorithm to compute the upper joint probability of a given instantiation induced by a given a Credal SPN \( S_w \) and a realization \( x \) of its variables. The algorithm visits nodes in topological reverse ordering, evaluating the following expression at...
We say that a CSPN is obtained by

\[ L^i(x, e) = \begin{cases} 
1 & \text{if } i \text{ is consistent,} \\
0 & \text{if } i \text{ is inconsistent,} \\
\prod_j L^j(x, e) & \text{if } i \text{ is a product,} \\
\max_{w_i \in C} \sum_{j \in ch(i)} w_{ij} L^j(x, e) & \text{if } i \text{ is a sum.}
\end{cases} \]

The desired value is obtained at the root of the network, that is, \( L^r(x, e) = \max_w S_w(x, e) \). Note that for selective credal SPNs, the sum in the last equation has at most one positive term.

### 4.1. Credal SPNs for Robustness Analysis

We can investigate the robustness of inferences drawn with a (precise) SPN by comparing the inferences produced by applying a perturbation to each weight in the network, while still respecting the normalization property. Given \( \epsilon \in (0, 1) \), the \( \epsilon \)-contamination of the vector \( u \) is the set:

\[ C_{u, \epsilon} = \left\{ (1 - \epsilon)u + \epsilon v : v \geq 0, \sum v_j = 1 \right\}. \]

We say that a CSPN is obtained by \( \epsilon \)-contamination of an SPN \( S_w \) if the weights associated with each sum node vary in the set obtained by the \( \epsilon \)-contamination of the weights in \( S \):

\[ \{ S_w : w_i \in C_{w, \epsilon}, i \text{ is a sum node} \}, \]

where \( w_i \) denotes the weights associated with sum node \( i \).

Alternatively, we can obtain a CSPN by varying the priors used for estimating the parameters of the SPN. Recall from Equation (2) that the weights of a selective SPN can be estimated as a Multinomial-Dirichlet model with counts \( N_j \), and prior strength \( s \). Thus, we can obtain a local credal set for a sum node \( i \) given a count vector \( N \) as:

\[ C_{N, \epsilon} = \left\{ w_i : w_{ij} = \frac{N_j + s \cdot v_i}{N_j + s}, v_j \geq 0, \sum v_j = 1 \right\}. \]

The equation above coincides with the Imprecise Dirichlet Model [36] for a (latent) RV representing the sum node \( i \), whose value "selects" which edge is active.

### 5. Robustness of MAP Inferences in SPNs

We can now provide an algorithm to obtain a CSPN by applying a perturbation to a (precise) SPN by comparing the inferences produced by

\[ \max \max_{x \neq x^*} \frac{S_w(x, e)}{S_w(x^*, e)} < 1. \]

Note that for SPNs (i.e., when \( C \) is a singleton) the problem reduces to deciding if there exists an instantiation \( x \) s.t. \( S(x, e) > S(x^*, e) \), Bodlaender et al. [3] showed that this problem is NP-hard for Bayesian networks; one can adapt their proof using ideas from [10] to show that deciding if an instance \( x^* \) is robust is NP-hard.

Before formulating an algorithm for deciding robustness of MAP inference, let us consider the simpler problem of computing the MAP instantiation with maximum joint probability over the set of induced SPNs. This will be used as a subroutine to verify robustness later. Thus consider a credal SPN \( \{ S_w : w \in C \} \) where \( C \) is given by the Cartesian product of sets \( C_i \) for each sum node \( i \), and some evidence \( e \). We are thus interested in computing

\[ \max_{x, w \in C} S_w(x, e). \]

Call a leaf node of the network a MAP leaf if its scope is in \( X \), otherwise call it an evidence leaf. The following algorithm computes the above quantity by traversing the network, calculating at each node \( i \):

\[ M^i = \begin{cases} 
1 & \text{if } i \text{ is consistent,} \\
0 & \text{if } i \text{ is inconsistent,} \\
\prod_{j \in ch(i)} M^j & \text{if } i \text{ is a product,} \\
\max_{w_i \in C_i} \max_{j \in ch(i)} w_{ij} M^j & \text{if } i \text{ is a sum node.}
\end{cases} \]

The definition of consistent and inconsistent nodes applies to leaf nodes and is identical to the one used to define the Max-Product algorithm. The soundness and complexity of the algorithm above are given by the following result.

**Theorem 1** Consider a selective CSPN \( \{ S_w : w \in C \} \) with root \( r \), where \( C \) is the Cartesian product of finitely-generated polytopes \( C_i \), one for each sum node \( i \). Then \( M^r \) computes \( \max_{x \in \operatorname{val}(X)} \max_{w \in C} S_w(x) \) in \( O(|S|) \) time, where \( |S| \) is the number of nodes and arcs in the model (assuming the local optimizations over the weights in \( M^i \) take linear time).

**Proof** We prove correctness by induction in the height \( h \) of \( S \). The base case of \( h=0 \) is immediate, as it consists of a leaf node which is maximized by setting the associated indicator to one, for the case of MAP leaves, or simply evaluated at the evidence. Assume that the inductive hypothesis is valid for networks of height \( h \geq 0 \) or smaller, and consider a network of height \( h+1 \) whose root is \( i \). Recall that in a selective SPN, at most one child \( j \) of a sum node satisfies \( S_j(x, e) > 0 \) for each instantiation \( x \). Let \( X_j \) denote the set of instantiations \( x \in \operatorname{val}(X) \) for which \( S_j(x, e) > 0 \). Then

\[ \max_{x \in \operatorname{val}(X)} \max_{w \in C} S_w^j(x, e) = \max_{j \in ch(i)} \max_{w_i \in C_i} w_{ij} S_w(x, e). \]

Thus, if \( i \) is a sum node, it follows that

\[ \max_{x} \max_{w \in C} S_w(x, e) = \max_{j \in ch(i)} \max_{w_i \in C_i} w_{ij} \max_{w \in C} S_w^j(x, e). \]
If \( i \) is a product node, we have that
\[
\max_x \max_w \prod_{j \in ch(i)} S_{w_j}^j(x) = \prod_{j \in ch(i)} \max_{w_j} \max_x S_{w_j}^j(x, e)
\]
\[
= \prod_{j \in ch(i)} M_j^i = M^i.
\]
The weights \( w_j \) in the first equation can be optimized independently for each \( j \in ch(i) \), and the disjointness of scopes for product nodes ensures that no weight is shared among the child sub-networks.

If we cache the values computed, then each node computes one value \( M^i \) in polynomial time in the number of edges of the network, considering that the local optimization over weights \( w_j \) is polynomial (which is the case for most sensible credal SPNs). Therefore the total cost of this computation is \( O(|S|) \).

The following algorithm decides if a MAP instantiation is robust, by traversing the network from the leaves to the root, computing, for each node \( i \):

\[
V^i = \begin{cases} 
1 & \text{if } i \text{ is consistent,} \\
0 & \text{if } i \text{ is inconsistent,} \\
\prod_j V^j & \text{if } i \text{ is a product node,} \\
\max_{j \in ch(i), j \neq k} U^j, V^k & \text{if } i \text{ is a sum node,}
\end{cases}
\]

where \( k \) is the active child of \( i \) for \( S \) at \( x^*, e \), and
\[
U^j = \max_{w_i \in \mathcal{E}_i, w_k \in \mathcal{L}^k(x^*, e)} \frac{w_j M^j}{w_k L^k(x^*, e)}.
\]

Where \( M^j \) and \( L^k \) was introduced at the previous section in equations 5 and 3 respectively.

The following result states the soundness and complexity of the algorithm for tree-shaped networks.

**Theorem 2** Consider a tree-shaped CSPN \( \{S_w : w \in \mathcal{C} \} \) with root \( r \), where \( \mathcal{C} \) is the Cartesian product of finitely-generated polytopes \( \mathcal{C}_i \), one for each sum node \( i \). Then \( V^r \) computes
\[
\max_x \max_w \left( \frac{S_w(x, e)}{S_w(x^*, e)} \right)
\]
in \( O(|S|) \) time, where \( |S| \) is the number of nodes and arcs in the model (assuming the optimizations over \( w_i \) in \( U_j \) can be performed in linear time).

**Proof** We prove that the algorithm is correct by induction in the height \( h \) of \( S \). The base case for \( h=0 \) is immediate. So assume that the inductive hypotheses is valid for networks of height \( h \geq 0 \) or smaller, and consider a network of height \( h+1 \) whose root is \( i \). Assume that \( i \) is a sum node. The tree shape of the network implies that the weights \( w_j \) that appear in a sub-network \( S_j^i \), \( j \in ch(i), j \neq i \), do not appear in any other sub-network \( S_{j'}^i \), \( j' \in ch(i), j' \neq j \). Denote by \( \mathcal{C}_j \) the subset of \( \text{val}(X) \) for which \( S_j^i(x, e) > 0 \). We have that
\[
\max_x \max_w \frac{S_w(x, e)}{w_k S_w(x^*, e)} = \max_x \max_w \frac{w_j \max_{x \in \mathcal{C}_j} S_w^j(x, e)}{w_k S_w^i(x, e)} = M^i.
\]
where \( k \) is the child of \( i \) for which \( S_k^i(x^*, e) > 0 \). For \( j = k \) it follows that
\[
\max_x \max_w \frac{w_j \max_{x \in \mathcal{C}_j} S_w^j(x, e)}{w_k S_w^i(x^*, e)} = \max_{w_i \in \mathcal{E}_i, w_j \in \mathcal{L}^k(x^*, e)} \frac{w_j M^i}{w_k L^k(x^*, e)} = U^j.
\]
If \( i \) is a product node then
\[
\max_x \max_w \left( \prod_j S_w^j(x) \right) = \max_{w_i \in \mathcal{E}_i} \prod_j S_w^j(x, e) = \prod_j \max_{w_i \in \mathcal{E}_i} \frac{S_w^j(x, e)}{S_w^j(x^*, e)} = \prod_j V^j = V^i.
\]
Computing \( V^i \) for a node \( i \) with the values of the children pre-computed and stored takes at most linear time in the number of children. Hence, the total cost of the computation is \( O(|S|) \).

The complexity of deciding robustness for multiply-connected CSPNs remains an open question.

### 6. Experiments

We evaluate the ability of our proposed method to distinguish between robust and non-robust MAP inferences in two different tasks. The first task requires learning a probabilistic model from complete data and then use that model to complete the missing values in the test data by maximizing the joint probability value of each instance. (this is also known as data imputation in the literature). We let \( X \) be the missing part and \( e \) the non-missing part. The second task considers multilabel classification, where objects are assignment multiple labels. This task can be solved by representing labels as a binary vector, \( X \), which can be
We learned selective SPNs from four well-known datasets
predicted by a probabilistic model of relevance labels $X$ given features $e$.

We learn selective SPNs for both tasks using the algorithm by Peharz et al. [23]. We then obtain CSPNs by either $\epsilon$-contamination (Equation (5)) or the Imprecise Dirichlet Model over the smoothed counts (Equation (6)). We use the CSPNs to determine the robustness of each MAP inference drawn with the (precise) SPN, and compare the performance of robust and non-robust classifications. We use a validation dataset to select values for $\epsilon$ and $s$ that maximizes the performance of robust inferences (according to some metric, as discussed later). We also compare our methods against a baseline robust analysis that compare the difference between the probability of the MAP instantiation and the second-best MAP instantiation (i.e., the second most probable configuration consistent with evidence). An instance is considered robust in this scheme if this difference is greater than a given threshold. We use a validation set to determine the best threshold for each dataset and task.

**Table 1: Characteristics of datasets used in completion tasks.**

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Train</th>
<th>Test</th>
<th>Evidence</th>
<th>Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNA</td>
<td>1600</td>
<td>1186</td>
<td>90</td>
<td>90</td>
</tr>
<tr>
<td>Jester</td>
<td>9000</td>
<td>4116</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>NLTCS</td>
<td>16181</td>
<td>3236</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>MSNBC</td>
<td>291326</td>
<td>58265</td>
<td>9</td>
<td>8</td>
</tr>
</tbody>
</table>

6.1. Completion

We learned selective SPNs for both tasks using the algorithm by Peharz et al. [23]. We then obtain CSPNs by either $\epsilon$-contamination (Equation (5)) or the Imprecise Dirichlet Model over the smoothed counts (Equation (6)). We use the CSPNs to determine the robustness of each MAP inference drawn with the (precise) SPN, and compare the performance of robust and non-robust classifications. We use a validation dataset to select values for $\epsilon$ and $s$ that maximizes the performance of robust inferences (according to some metric, as discussed later). We also compare our methods against a baseline robust analysis that compare the difference between the probability of the MAP instantiation and the second-best MAP instantiation (i.e., the second most probable configuration consistent with evidence). An instance is considered robust in this scheme if this difference is greater than a given threshold. We use a validation set to determine the best threshold for each dataset and task.

**Table 1:** Characteristics of datasets used in completion tasks.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Train</th>
<th>Test</th>
<th>Evidence</th>
<th>Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNA</td>
<td>1600</td>
<td>1186</td>
<td>90</td>
<td>90</td>
</tr>
<tr>
<td>Jester</td>
<td>9000</td>
<td>4116</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>NLTCS</td>
<td>16181</td>
<td>3236</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>MSNBC</td>
<td>291326</td>
<td>58265</td>
<td>9</td>
<td>8</td>
</tr>
</tbody>
</table>

For each metric, we select the values for $\epsilon^*$, $s^*$ and the probability difference $p^*$ by maximizing the performance of the robust instances on the validation set (according to some criterion). These values are kept fixed during evaluation in the test set.

The results are shown in Table 2, where $\epsilon^*$, $s^*$ and $p^*$ stand for $\epsilon$-contamination, IDM and probability difference criterion, with the parameters and threshold selected using a validation set, as described. The best performing method for each dataset and partition is shown in boldface. We omit the results for the DNA dataset, as all instances had more than on MAP instantiation, making all inferences non-robust by any of the criteria.

According to the results, $\epsilon$-contamination outperforms all other methods in terms of both Hamming Score and Exact Match. It also achieves the highest discrepancy between the performance of robust and non-robust predictions. IDM is outperformed by the other methods in two datasets.

Figure 3 shows the test-set performance of robust instances in the test set as for different values of $\epsilon$, $s$ and different thresholds for probability difference. The curves with green triangle marks shown Exact Match, while the curves in orange square marks denote Hamming scores. We see that $\epsilon$-contamination improves performance as the value of $\epsilon$ is increased, while the correlation of the threshold for probability difference and accuracy is less clear. IDM obtains intermediary results. All three approaches perform similarly at the highest values.

6.2. Multilabel Classification

We perform the robustness analysis of predictions on 10 benchmark of multilabel classification domains. Table 3 shows general characteristics of the datasets used: domain, number of features $M$, number of instances $N$, number of labels $L$, label cardinality $LC = \frac{1}{N} \sum_{i=1}^{N} |x_i|$ and label density $LD = \frac{1}{N} \sum_{i=1}^{N} |x_i|$, where $|x|$ returns the number of ones in the instantiation $x$.

In addition to Exact Match, we also evaluate multilabel classifications by a common measure $[12, 13]$, which rewards relevant predictions while discounting for irrelevant predictions. We name this metric **Accuracy (Acc)**, and compute it as:

$$\text{Acc} = \frac{1}{N} \sum_{i=1}^{N} \frac{|x_i^* \land \hat{x}_i|}{|x_i^* \lor \hat{x}_i|},$$

where again $N$ is the test dataset size, $x^*$ is the MAP inference and $\hat{x}$ the true labels. The operations $\land$ (resp. $\lor$) treat as boolean values.
Table 2: Results for completion tasks, \( \%I \) column shows instances percentage, \( \Delta EM \) and \( \Delta HS \) is the metric difference between Robust and \( \sim \)Robust subsets.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Exact Match</th>
<th>Hamming Score</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Robust ( %I )</td>
<td>( \sim )Robust ( %I )</td>
</tr>
<tr>
<td>Jester</td>
<td>( \varepsilon^* )</td>
<td>0.259</td>
</tr>
<tr>
<td></td>
<td>( s^* )</td>
<td>0.076</td>
</tr>
<tr>
<td></td>
<td>( p^* )</td>
<td>0.016</td>
</tr>
<tr>
<td>NLTCS</td>
<td>( \varepsilon^* )</td>
<td>0.736</td>
</tr>
<tr>
<td></td>
<td>( s^* )</td>
<td>0.736</td>
</tr>
<tr>
<td></td>
<td>( p^* )</td>
<td>0.736</td>
</tr>
<tr>
<td>MSNBC</td>
<td>( \varepsilon^* )</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>( s^* )</td>
<td>0.464</td>
</tr>
<tr>
<td></td>
<td>( p^* )</td>
<td>0.727</td>
</tr>
</tbody>
</table>

Figure 3: Test-set performance vs. threshold for completion tasks. Each row displays results for a dataset. From the top to bottom row: Jester, NLTCS, MSNBC. The curves with green triangle marks shown Exact Match, while the curves in orange square marks denote Hamming scores.
Table 3: Multi-Label Datasets, their domains, size of their feature vector (M), number of instances (N), number of labels (L), label cardinality (LC) and label density (LD).

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Domain</th>
<th>M</th>
<th>N</th>
<th>L</th>
<th>LC</th>
<th>LD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arts-Yahoo</td>
<td>Text</td>
<td>500</td>
<td>7484</td>
<td>26</td>
<td>1.65</td>
<td>0.06</td>
</tr>
<tr>
<td>Business-Yahoo</td>
<td>Text</td>
<td>500</td>
<td>11214</td>
<td>30</td>
<td>1.6</td>
<td>0.05</td>
</tr>
<tr>
<td>CAL500</td>
<td>Music</td>
<td>68</td>
<td>502</td>
<td>174</td>
<td>26.04</td>
<td>0.15</td>
</tr>
<tr>
<td>Emotions</td>
<td>Music</td>
<td>72</td>
<td>593</td>
<td>6</td>
<td>1.87</td>
<td>0.31</td>
</tr>
<tr>
<td>Flags</td>
<td>Images</td>
<td>19</td>
<td>194</td>
<td>7</td>
<td>3.39</td>
<td>0.48</td>
</tr>
<tr>
<td>Health-Yahoo</td>
<td>Text</td>
<td>500</td>
<td>9205</td>
<td>32</td>
<td>1.64</td>
<td>0.05</td>
</tr>
<tr>
<td>Human</td>
<td>Biological</td>
<td>440</td>
<td>3106</td>
<td>14</td>
<td>1.19</td>
<td>0.08</td>
</tr>
<tr>
<td>Plant</td>
<td>Biological</td>
<td>440</td>
<td>978</td>
<td>12</td>
<td>1.08</td>
<td>0.09</td>
</tr>
<tr>
<td>Scene</td>
<td>Images</td>
<td>294</td>
<td>2407</td>
<td>6</td>
<td>1.07</td>
<td>0.18</td>
</tr>
<tr>
<td>Yeast</td>
<td>Biological</td>
<td>103</td>
<td>2417</td>
<td>14</td>
<td>4.24</td>
<td>0.3</td>
</tr>
</tbody>
</table>

denote the vector obtained by coordinate-wise minimum (resp. maximum) of the instances. We do not use Hamming Score, as it does not distinguish between correct prediction of presence and absence of labels, and can lead to overoptimistic measures when the number of labels is high and label density is low.

Similar to the previous task, we select the best values \( \varepsilon^*, s^* \) and \( p^* \) using the validation dataset, and then perform a robustness analysis for each multilabel prediction in the test dataset. The results are summarized in Table 4. All instances in the CAL500 dataset contained more than one MAP instantiation and are therefore deemed non-robust by all methods. We omit these results from the table.

One sees from these results that the CSPNs obtained by IDM achieve the highest accuracy in 5 of the 9 domains, followed by the CSPNs obtained with \( \varepsilon \)-contamination (3 out of 9). Probability difference outperforms the other methods with respect to accuracy only for Human, where the CSPN-based methods consider all instances robust. Yet, the difference in accuracy (or exact match scores) for robust and non-robust is very small, showing that the two sets perform indeed very similar (but perhaps it would be more sensible to classify all instances as non-robust by all methods). We omit these results from the table.

One sees from these results that the CSPNs obtained by IDM achieve the highest accuracy in 5 of the 9 domains, followed by the CSPNs obtained with \( \varepsilon \)-contamination (3 out of 9). Probability difference outperforms the other methods with respect to accuracy only for Human, where the CSPN-based methods consider all instances robust. Yet, the difference in accuracy (or exact match scores) for robust and non-robust is very small, showing that the two sets perform indeed very similar (but perhaps it would be more sensible to classify all instances as non-robust). The IDM-based CSPNs perform particularly poorly in the Arts domain, where the accuracy of the robust portion is significantly inferior to the accuracy in the non-robust portion. We conjecture that this is due to some peculiarity of the learned network, but were not able to provide any deep explanation at this point.

Regarding Exact Match, we see that IDM-based CSPNS outperform other methods in 4/9 of the domains, while probability difference achieves the best performance in 3/9 of domains. CSPNs based on \( \varepsilon \)-contamination are outperformed in all but one domain (Arts), where IDM-based results exhibit the same strange behavior (robust instances obtain worse results than non-robust instances). One possible explanation for the best performance of \( \varepsilon \)-contamination is that it is more conservative, assigning more instances to the non-robust portion; this is particularly beneficial under exact match, which is more strict with mistakes.

7. Conclusion

Sum-Product Networks (SPNs) are deep probabilistic models that have shown very promising results in several tasks. Selective SPNs are a subclass of models that allows tractable MAP inference with only a small decrease in accuracy. In this work, we presented polynomial-time algorithm for robust analysis of MAP inference in tree-shaped selective SPNs. We evaluated our algorithms in two different tasks: completing missing values and performing multilabel classification. Our results show that the proposed algorithm is better at discrimination of robust and non-robust inferences than the standard approach based on the difference of probabilities. We left for the future the analysis of the complexity of robustness for multiply-connected SPNs, as well as a more extensive empirical evaluation.

Acknowledgments

We thank Robert Peharz for kindly sharing the source code of the Selective SPN learning algorithm. This study was financed in part by the Brazilian Agency Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) - Finance Code 001. The second author also received financial support from CNPq grants no. 303920/2016-5 and 420669/2016-7.

References


### Table 4: Results for Multilabel classification, %I column shows instances percentage, $\Delta EM$ and $\Delta HS$ is the metric difference between Robust and ¬Robust subsets

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Accuracy</th>
<th>Exact Match</th>
<th>$\Delta EM$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$Robust$</td>
<td>%I</td>
<td>¬Robust</td>
</tr>
<tr>
<td>Arts</td>
<td>$e^*$</td>
<td>0.88</td>
<td>1.2</td>
</tr>
<tr>
<td></td>
<td>$s^*$</td>
<td>0.107</td>
<td>51.94</td>
</tr>
<tr>
<td></td>
<td>$p^*$</td>
<td>0.81</td>
<td>6.95</td>
</tr>
<tr>
<td>Business</td>
<td>$e^*$</td>
<td>0.751</td>
<td>72.73</td>
</tr>
<tr>
<td></td>
<td>$s^*$</td>
<td>0.781</td>
<td>45.32</td>
</tr>
<tr>
<td></td>
<td>$p^*$</td>
<td>0.762</td>
<td>68.4</td>
</tr>
<tr>
<td>Emotions</td>
<td>$e^*$</td>
<td>0.595</td>
<td>17.65</td>
</tr>
<tr>
<td></td>
<td>$s^*$</td>
<td>0.686</td>
<td>10.92</td>
</tr>
<tr>
<td></td>
<td>$p^*$</td>
<td>0.574</td>
<td>28.57</td>
</tr>
<tr>
<td>Flags</td>
<td>$e^*$</td>
<td>0.917</td>
<td>10.53</td>
</tr>
<tr>
<td></td>
<td>$s^*$</td>
<td>0.917</td>
<td>10.53</td>
</tr>
<tr>
<td></td>
<td>$p^*$</td>
<td>0.917</td>
<td>10.53</td>
</tr>
<tr>
<td>Health</td>
<td>$e^*$</td>
<td>0.667</td>
<td>0.11</td>
</tr>
<tr>
<td></td>
<td>$s^*$</td>
<td>0.637</td>
<td>47.88</td>
</tr>
<tr>
<td></td>
<td>$p^*$</td>
<td>0.655</td>
<td>4.72</td>
</tr>
<tr>
<td>Human</td>
<td>$e^*$</td>
<td>0.203</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>$s^*$</td>
<td>0.203</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>$p^*$</td>
<td>0.211</td>
<td>42.6</td>
</tr>
<tr>
<td>Plant</td>
<td>$e^*$</td>
<td>0.331</td>
<td>37.76</td>
</tr>
<tr>
<td></td>
<td>$s^*$</td>
<td>0.367</td>
<td>47.96</td>
</tr>
<tr>
<td></td>
<td>$p^*$</td>
<td>0.345</td>
<td>36.22</td>
</tr>
<tr>
<td>Scene</td>
<td>$e^*$</td>
<td>0.857</td>
<td>5.83</td>
</tr>
<tr>
<td></td>
<td>$s^*$</td>
<td>0.929</td>
<td>2.92</td>
</tr>
<tr>
<td></td>
<td>$p^*$</td>
<td>0.923</td>
<td>5.42</td>
</tr>
<tr>
<td>Yeast</td>
<td>$e^*$</td>
<td>0.436</td>
<td>5.79</td>
</tr>
<tr>
<td></td>
<td>$s^*$</td>
<td>0.436</td>
<td>5.79</td>
</tr>
<tr>
<td></td>
<td>$p^*$</td>
<td>0.425</td>
<td>97.93</td>
</tr>
</tbody>
</table>


Heinrich Jiang, Been Kim, Melody Guan, and Maya Gupta. To trust or not to trust a classifier. In Advances in Neural Information Processing Systems, 2018.


