Safety Augmentation in Decision Trees

Prof. Pallab Dasgupta
Sumanta Dey
Briti Gangopadhyay
Indian Institute of Technology Kharagpur, India

Authors

Dr. Pallab Dasgupta
AK Singh Distinguished Chair Professor in AI
Dept of Computer Sc. and Engg.
IIT Kharagpur
Research Interest: Artificial Intelligence, Machine Learning and Formal Verification

Sumanta Dey
Research Scholar
Dept of Computer Sc. and Engg.
IIT Kharagpur
Research Interest: Safety assurance of machine learning models by formal verification

Briti Gangopadhyay
Research Scholar
Dept of Computer Sc. and Engg.
IIT Kharagpur
Research Interest: Neuro-Symbolic Artificial Intelligence, Safe Autonomous Driving.

Introduction to Decision Trees

What is Decision Tree?

- **Tree like Structure**
  - -Inner Nodes contains the Attributes values
  - -Leaf Nodes contains the Decision Values

- **Old, Well Known and Widely Used ML model**

- **Interpretable Models**
  - Hence Easy to Verify
    - Thus Makes it suitable for using in Safety Critical Domain

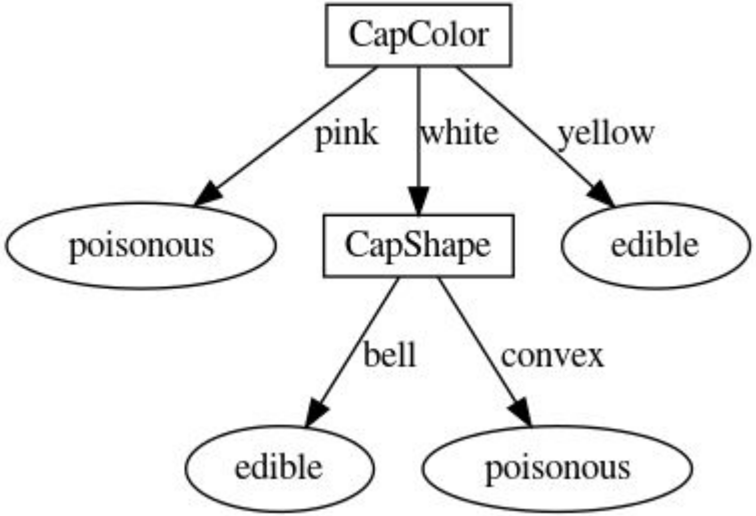


Figure 1: This figure represents a Decision Tree that classify a mushroom edible/poisonous[1] based on it's Cap Color and Cap Shape.

[1] Dheeru Dua and Casey Graff. UCI machine learning repository, 2017.

Learning Decision Tree

- Finding an Optimal Decision Tree (with minimum height) is **NP Complete Problem**[2]**.**
- **Greedy Approach** gives **Sub Optimal** Decision Tree

Ex:

ID3 (Iterative Dichotomiser 3)[3] **Algorithm**:

A Greedy approach orders the nodes based on decreasing order of Information Gain.

- *Information Gain(S|A) = Entropy(S) - Entropy(S|A)*
- *Entropy(S) = ∑(-1)*p(x)*log(p(x))*

[2] Hyafil Laurent and Ronald L Rivest.Constructing optimal binary decision trees is np-complete.Information processing letters, 5(1):15–17,1976.
[3] J. Ross Quinlan. Induction of decision trees.Machine learning, 1(1):81–106, 1986.

Safety Augmentation in Decision Trees

Why Required?

- Noise
- Missing Data

Ex:

CapShape	CapColor	GillColor	Poisonous
Bell	Pink	Green	Poisonous
Bell	Pink	White	Poisonous
Bell	Pink	Gray	Poisonous
Convex	Pink	Gray	Poisonous
Convex	Pink	Brown	Poisonous
Convex	White	Brown	Poisonous
Convex	White	White	Poisonous
Convex	White	Gray	Poisonous
Convex	Yellow	Brown	Edible
Convex	Yellow	Gray	Edible
Convex	Yellow	White	Edible
Bell	Yellow	White	Edible
Bell	Yellow	Gray	Edible
Bell	Yellow	Brown	Edible
Bell	White	Brown	Edible
Bell	White	Gray	Edible
Bell	White	White	Edible

Table 1: Mushroom dataset

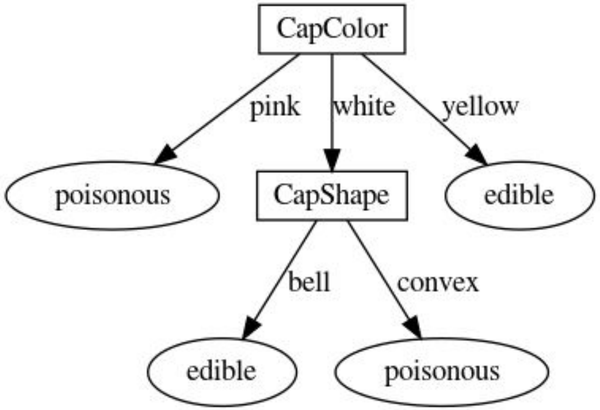


Figure 2: Decision Tree created from the table data using ID3 Algorithm

Suppose Safety requirements gleaned from (non-statistical) domain knowledge:

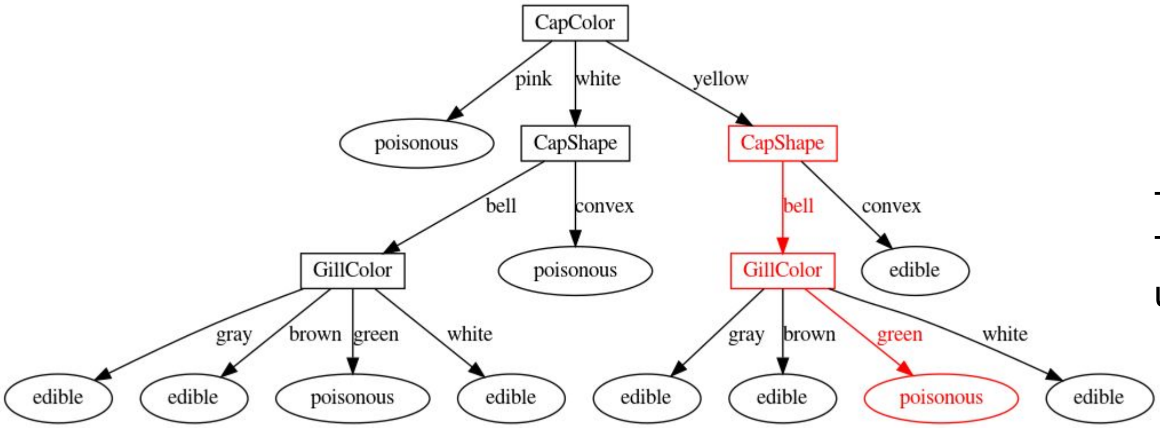
$$(CapShape = bell \wedge GillColor = green) \Rightarrow Poisonous$$

Contradicting with Decision Tree (Figure 2) Decision

Post-Facto Safety Augmentation

Method:

1. **Step 1:** Build the Decision Tree
2. **Step 2:** Analyze safety assertions
   a. Analyze safety assertions before using the decision tree.
      - Safety-critical scenarios often have specific attributes which need not be examined if the decision is safe anyway.
   b. Analyze safety assertions after using the decision tree.
      - Modify the decision tree branches according to the safety assertions



The resulting Decision Tree may become unnecessarily **complex.**

Figure 3: Decision Tree after incorporating the Safety Property

Dataset Augmentation

- Explicit (Generating Support Dataset)
- Implicit (Without generating Support Dataset)

Explicit Dataset Augmentation(Generating Support Dataset):

- Add the missing support dataset

CapShape	CapColor	GillColor	Poisonous
Bell	White	Green	Poisonous
Bell	Yellow	Green	Poisonous

- Then use ID3 algorithm.
- Don't select the decision node value based on the **majority count.**

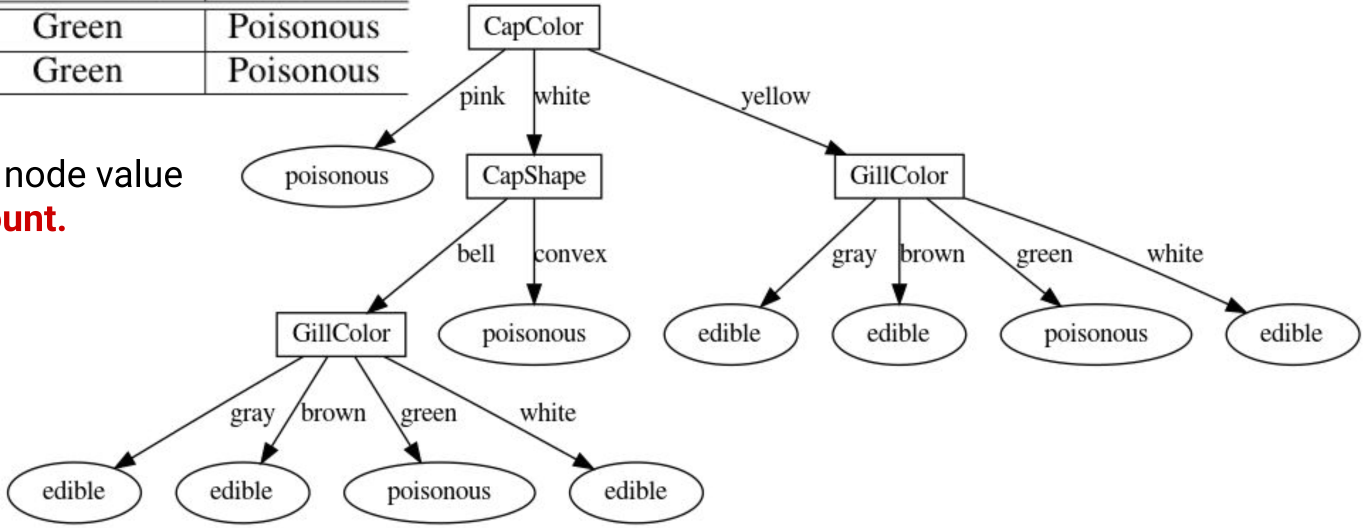


Figure 4: Decision Tree generated from the Augmented Dataset

Implicit Dataset Augmentation

- Only **class counts** are required to calculate the Information Gain.
- Safety Assertion with large support dataset requires lots of **computation to generate**.

To calculate Information Gain (IG) including Safety Assertion Support Dataset:

1. Consider Support Dataset Count [*S(i|t)*] in class-*i* count at branch *t*

   $N(i|t) = R(i|t) + S(i|t)$ Where, *R(i|t)* is class-*i* count at branch t in input dataset

2. Then use that count to calculate class-*i* probability, which is required to calculate Entropy and IG

$$p(i|t) = \frac{N(i|t)}{\sum_{j=1}^{k} N(j|t)} = \frac{N(i|t)}{N(t)}$$

Implicit Dataset Augmentation - Benefits/Side Effects

Advantages:

1. Generate similar Decision Tree, however, faster than Explicit Dataset Augmentation.

2. Generate smaller Decision Tree than Post-Facto Augmentation.

Disadvantages:

1. Introduces unnecessary bias.

   Ex: The missing support dataset of the safety assertion $(CapShape = bell \wedge GillColor = green) \Rightarrow Poisonous$ from the input dataset Table 1: Mushroom Dataset.

CapShape	CapColor	GillColor	Poisonous
Bell	White	Green	Poisonous
Bell	Yellow	Green	Poisonous

   This need not be true, and in nature, we may not have a mushroom of yellow CapColor, which has a bell like CapShape and green GillColor.

Multi Assertion Safety Augmentation

Scenarios needs to be taken care for Multi Assertion Safety Augmentation:

1. **Assertions with the same consequent:**
   Take union of the support datasets count.

2. **Assertions with different consequents:**
   Ensure the assertions are disjoint.

3. **Causal versus Diagnostic Assertions:**
   Convert the causal form and then used in our methodology.

   For Ex:
   The Causal Rule:
   $Cavity \Rightarrow Toothache$
   can be rewritten as a

   Diagnostic Rule:
   $\neg Toothache \Rightarrow \neg Cavity.$

Experimental Results

Dataset	ID	Assertion
Breast Cancer	1	$(Age = (30\text{-}39) \wedge Tumor\text{-}Size = (30\text{-}34) \wedge Irradiation = Yes) \Rightarrow Recurrence\text{-}Events$
Mushroom	1	$(Cap\text{-}Shape = Bell \wedge Gill\text{-}Color = Green) \Rightarrow Poisonous$
	2	$(Stalk\text{-}color\text{-}above\text{-}ring = Bell \wedge Stalk\text{-}color\text{-}below\text{-}ring = Green) \Rightarrow Poisonous$
Nursery	1	$(Student\text{-}Health = Not\text{-}Recommended) \Rightarrow Not\text{-}Recommended$
Tic-Tac-Toe	1	$(top\text{-}left\text{-}square = o \wedge top\text{-}middle\text{-}square = o \wedge top\text{-}right\text{-}square = o) \Rightarrow x\text{-}losses$
	2	$(middle\text{-}left\text{-}square = o \wedge middle\text{-}middle\text{-}square = o \wedge middle\text{-}right\text{-}square = o) \Rightarrow x\text{-}losses$
	3	$(bottom\text{-}left\text{-}square = o \wedge bottom\text{-}middle\text{-}square = o \wedge bottom\text{-}right\text{-}square = o) \Rightarrow x\text{-}losses$

Table 2: Assertions for Benchmark Datasets[4]

Dataset	Prop ID	Original Decision Tree			Post-facto Safety Augmentation			Integrated Safety Augmentation		
		Depth	Total Nodes	Runtime (Sec)	Depth	Total Nodes	Runtime (Sec)	Depth	Total Nodes	Runtime (Sec)
Breast Cancer	1	8	179	0.014	8	202	0.001	7	181	0.012
Mushroom	1	5	29	0.284	7	281	0.002	6	60	0.346
	2	5	29	0.284	7	281	0.002	6	36	0.375
Nursery	1	9	803	0.275	9	803	0.001	9	803	0.260
Tic-Tac-Toe	1	8	343	0.034	8	343	0.001	8	318	0.035
	2	8	343	0.034	10	463	0.002	8	363	0.036
	3	8	343	0.034	10	514	0.002	8	310	0.035

Table 3: Comparison of runtimes and dimensions of decision trees

[4] Dheeru Dua and Casey Graff. UCI machine learning repository, 2017.

Conclusion

- Safety augmentation is necessary when the learned function is used in a safety critical context.

- We present the first methodology for safety augmentation in decision trees where the safety requirement is expressed in terms of assertions.

- Our results indicate that augmenting the information gain metrics yields safe decision trees which are considerably smaller than ones obtained by post-facto safety augmentation.

Questions?

Thank You!