# SAVEETHA SCHOOL OF ENGINEERING

## SIMATS, CHENNAI - 602105

# CSA1350-THEORY OF COMPUTATION FOR PUMPING LEMMA

Team Details :

1 . P. Harsha Vardhan Reddy (192210047)
2 . Y. Abhishek (192210121)
3 . P. Dinesh Karthik (192210043)
4. N. Sanjay (192210226)

# SPAM CLASSIFICATION

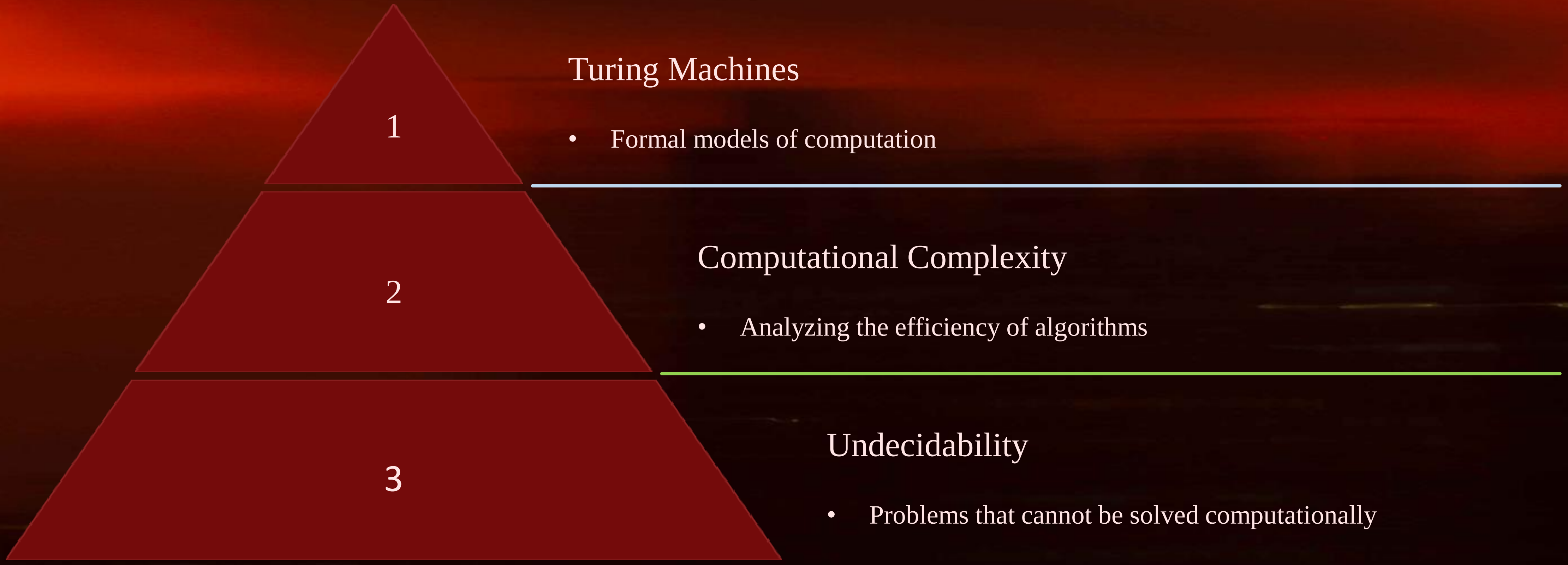
# Introduction to Spam Classification

- Spam Classification is the process of identifying and filtering out unwanted or unsolicited messages, commonly referred to as spam, from legitimate communication. This is particularly important for email systems, social media platforms, and online forums to ensure the quality and security of information flow.

- Spam refers to unsolicited, irrelevant, or inappropriate messages sent over the internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.

- Spam classification is a crucial task in modern email and communication systems. By accurately identifying and filtering out unwanted, unsolicited messages, users can maintain a clean and focused inbox, improving productivity and digital well-being.

# Fundamentals of Theory of Computing



Turing Machines

- Formal models of computation

Computational Complexity

- Analyzing the efficiency of algorithms

Undecidability

- Problems that cannot be solved computationally

- Theory of computing is the foundational discipline that underpins our understanding of what can and cannot be computed by machines. Key concepts include Turing machines as models of computation, the analysis of computational complexity, and the study of undecidable problems that lie beyond the reach of algorithms.

# The Spam Classification Problem

1

### Email Deluge

- Dealing with the overwhelming volume of emails received daily

2

### Fraudulent Content

- Identifying malicious messages containing scams, phishing, or malware

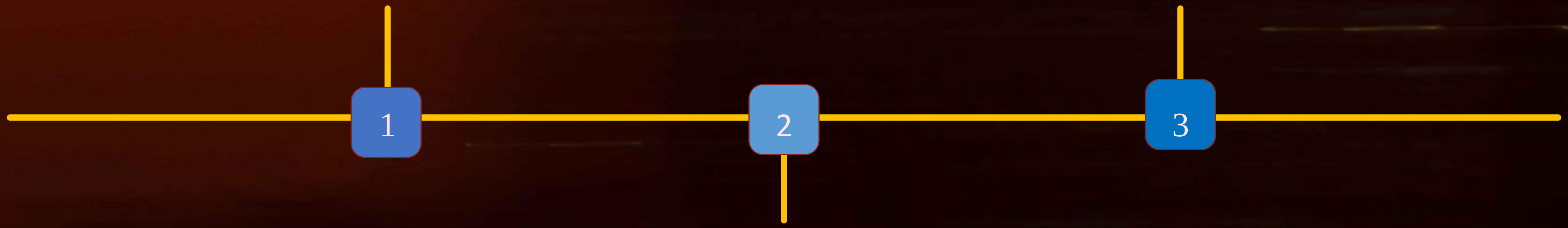
3

### Protecting Inboxes

- Filtering out unwanted spam to maintain a clean, organized inbox

- The spam classification problem involves developing intelligent systems to automatically sort through the vast influx of emails and separate legitimate messages from unwanted, malicious spam. This is a crucial task to safeguard users' inboxes, prevent financial losses, and maintain productivity in the face of increasingly sophisticated spam tactics.

# Feature Engineering for Spam Classification



## Text Preprocessing

Clean and normalize email text by removing HTML tags, URLs, punctuation, and converting to lowercase. This helps the model focus on relevant content.

## Lexical Features

Extract features like word counts, character counts, and the presence of trigger words associated with spam. These provide insight into the writing style.

## Semantic Features

Use natural language processing to analyze email content for sentiment, topics, and other semantic characteristics that distinguish spam from legitimate messages.

# Computational Complexity of Spam Classification

1

## Polynomial-Time Algorithms

- Many spam classification algorithms, such as naive Bayes and logistic regression, are known to have polynomial-time complexity, making them efficient for practical use.

2

## NP-Hardness Challenges

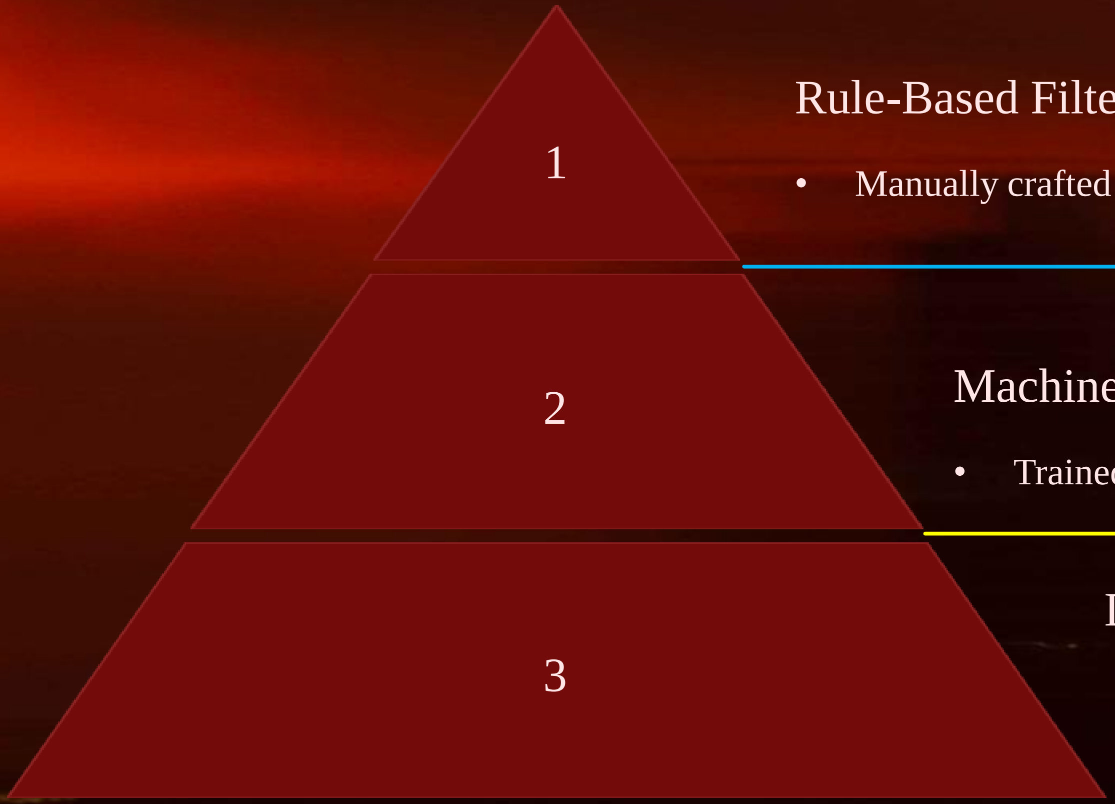
- However, certain variants of the spam classification problem, such as those involving adversarial attacks, have been shown to be NP-hard, posing computational challenges.

3

## Tradeoffs and Approximations

- Researchers often explore tradeoffs between classification accuracy and computational complexity, as well as approximate algorithms to tackle the NP-hard aspects of spam classification.

# Algorithmic Approaches to Spam Classification



### Rule-Based Filtering

- Manually crafted rules to identify spam

### Machine Learning Models

- Trained on labeled spam/ham data

### Deep Learning Architectures

- Leverage neural networks for advanced feature extraction

- Spam classification has been approached using a variety of algorithmic techniques. Traditional rule-based filters rely on manually curated heuristics to identify spam messages. More advanced approaches leverage machine learning models, including linear classifiers, decision trees, and ensemble methods, trained on large datasets of labeled spam and ham emails. The cutting edge of spam filtering utilizes deep neural networks that can automatically extract rich features from email content and metadata.

# Spam Classification using Naive bayes Algorithm

- Naive Bayes is a probabilistic classifier based on Bayes' Theorem with the assumption of independence between features. It is particularly effective for text classification tasks like spam detection.

- Naive Bayes is a probabilistic classifier based on Bayes' Theorem with the "naive" assumption that the features are conditionally independent given the class label. It is particularly popular for text classification tasks such as spam detection. Here is a step-by-step explanation of how Naive Bayes can be used for spam classification, including the relevant formulae.

- Why Naive Bayes?
  Simplicity: Easy to implement and understand.
  Efficiency: Requires less computational resources.
  Effectiveness: Works well with text data, especially when the feature set is large.

- Formulae:

- $P(C/X)=P(X/C).P(C)/P(X)$

- $P(C)$= Number of documents in class C/Total number of documents

- $P(X)$=Number of variables/total classes

# Evaluation Metrics and Benchmarking

1

### Accuracy

- Measures the overall correctness of the classifier

2

### Precision

- Identifies the proportion of true positives among all positive predictions

3

### Recall

- Captures the proportion of true positives identified out of all actual positives

4

### F1-Score

- Balances precision and recall into a single metric

- Evaluating the performance of spam classification models is crucial to ensure they are effective and reliable. Key metrics include accuracy, precision, recall, and the F1-score, which provide insights into the classifier's ability to correctly identify spam and non-spam messages. Benchmarking against industry standards and cross-validating results help validate the model's generalization capabilities.

# Limitations and Challenges

1

### Evolving Spam Tactics

- Spammers are constantly devising new techniques to bypass spam filters, making it an ongoing battle to stay ahead of their tactics.

2

### Data Imbalance

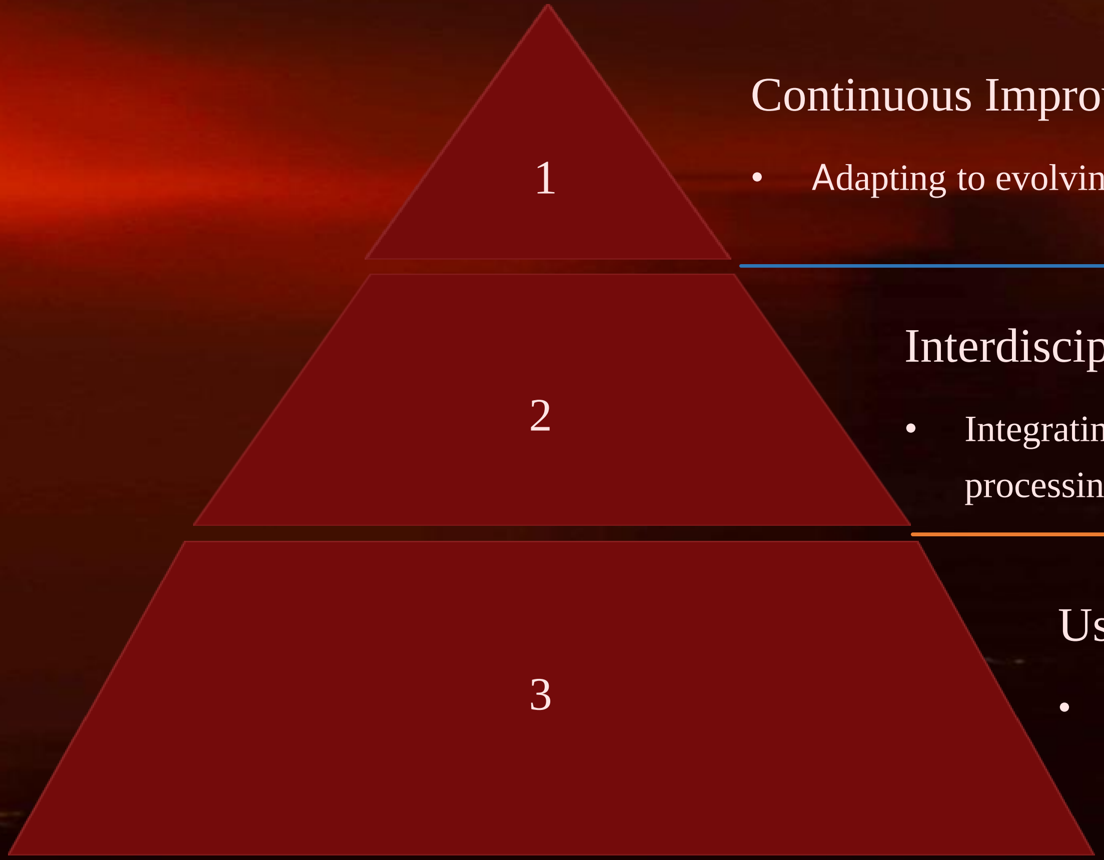
- Spam classification often suffers from highly imbalanced datasets, with legitimate emails vastly outnumbering spam messages, making it challenging to train effective models.

3

### Context Dependency

- The meaning and intent of emails can be highly context-dependent, making it difficult for algorithms to accurately distinguish between spam and legitimate messages.

# Conclusion and Future Directions



### Continuous Improvement

- Adapting to evolving spam tactics

### Interdisciplinary Collaboration

- Integrating advances in machine learning, natural language processing, and cryptography

### User-Centric Design

- Enhancing the spam classification experience for end-users

- In conclusion, spam classification remains an active area of research and development, requiring continuous innovation to stay ahead of evolving spam tactics. Future advancements will likely involve deeper interdisciplinary collaboration, leveraging the latest breakthroughs in machine learning, natural language processing, and cryptography. Ultimately, the goal is to deliver a seamless, user-centric spam classification experience that protects individuals and organizations from the ever-growing threat of unwanted and malicious messages.

# THANK YOU