Combinatorial Methods for Artificial Intelligence

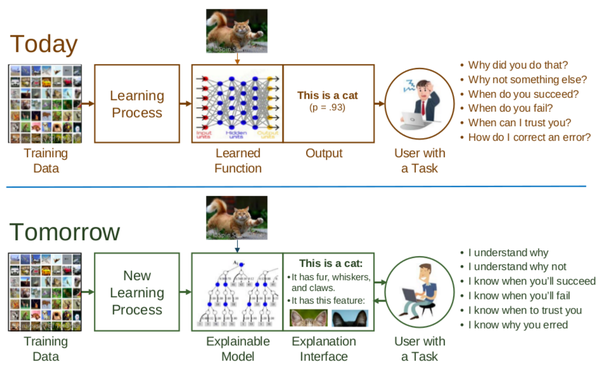
Dimitris E. Simos, Bernhard Garn, Dominik-Philip Schreiber,
Ludwig Kampel, Rick Kuhn, Raghu Kacker

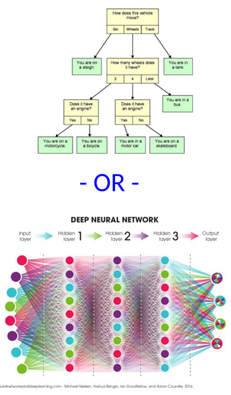
COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

SBA Research

MATRIS

Combinatorial Methods for Explainable Artificial Intelligence (XAI)

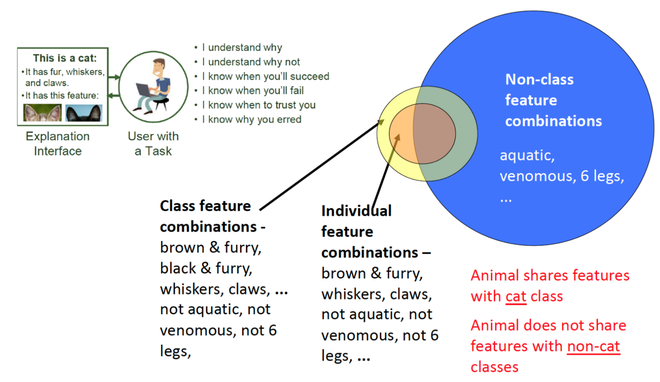




Expert system:
Good for explanations,
not so good for accuracy

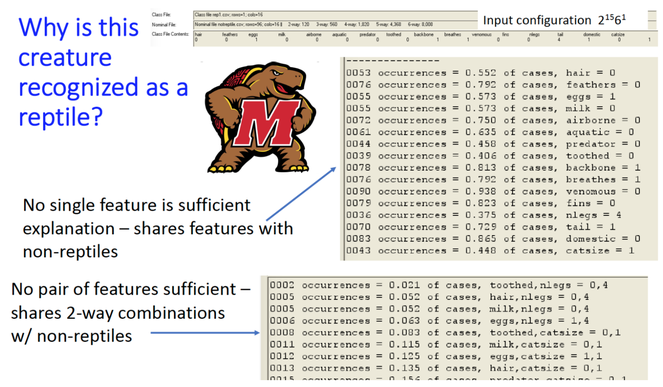
Neural nets:
Good for accuracy,
not so good for explanations

How do we get the best of both worlds?



Combinatorics for XAI

Why is this creature recognized as a reptile?

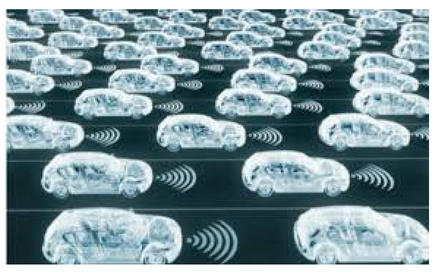


- Only reptiles have these 3-way combinations of features:
  - not aquatic AND not toothed AND four legs
  - egg-laying AND not aquatic AND four legs
  - not hairy AND four legs AND cat size
  - not milk-producing AND not aquatic AND four legs
  - not milk-producing AND four legs AND cat size
  - not predator AND not toothed AND four legs

Intelligent Virtual Assistants (IVAs)

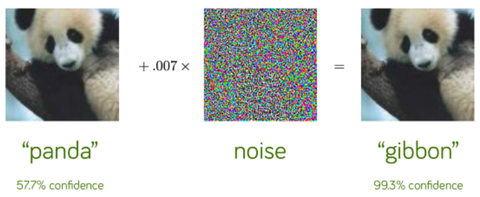
- Vulnerabilities and exploits demonstrated against available IVA platforms.
- Exhibit large new attack surface due to functionality.
- Need all-embracing novel security and reliability testing (e.g., explainable AI).

Autonomous Vehicles



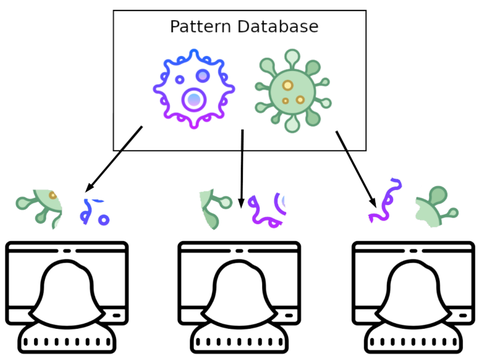
- Connected, intelligent, and autonomous vehicles pose new safety and security challenges.
- Systematic and holistic safety and security approach required to test networked computers on wheels.
- Guaranteeing the reliability and robustness is a major challenge.

Generative Adversial Networks (GANs)



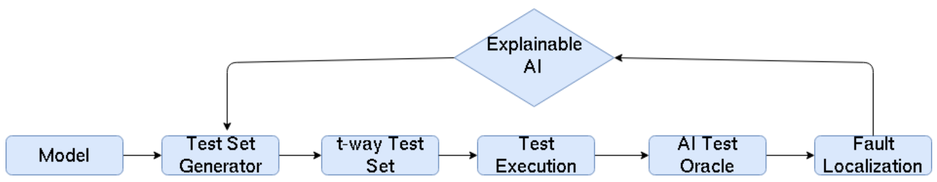
- Combinatorial methods to reduce number of queries to targeted classifier.
- Generating inputs that get misclassified by different classification networks.

AI-based Combinatorial Computer Virology



- Most anti-virus scan patterns can easily be extracted from anti-virus software.
- Using balanced incomplete block designs and AI to generate effective subsets of malware patterns.
- Prevent black-box analysis by only using specific subset per user for malware detection.
- Single user cannot learn full detection pattern.

Analyzing AI-based Test Oracles



- Software and security testing scenarios.
- Test oracles can contain and use AI-systems.
- Approach finds the root cause of security vulnerabilities.
- Provides transparency and explanations for test outcomes.

D. R. Kuhn, R. N. Kacker, Y. Lei, and D. E. Simos. Combinatorial Methods for Explainable AI. In *2020 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, 2020. to appear.

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.