The 2023 IARIA Annual Congress on Frontiers in Science, Technology, Services, and Applications (IARIA Congress 2023)

The Triumvirate of Bespoke Diverse Hybridized Activation Functions, Adaptive Momentum, and Enhanced Entropic Wavelet Energy Spectrum Discernment for Higher Efficacy Detection of Artificial Intelligence-centric Attacks

Steve Chan
schan@dengineering.org

Ill-Conditioned Optimization Problems

(a.k.a., “Narrow Canyon Facilitation”)

Higher Efficacy Detection of Artificial Intelligence Attacks (AIA)

1. Diverse hybridized Activation Functions (AFs)

+

2. Bespoke Nonlinear Conjugate Gradient (NCG)/
Nesteror Accelerated Gradient (NAG)
for Adaptive Momentum (ADaM)

+

3. Second-Order Cone Programming Relaxations (SOCPR) for Entropic Wavelet Energy Spectrum (EWES) Discernment (ED)

Table of Contents

Higher Efficacy Detection of AIA

Table of Contents:

- Introduction……Slides 6-9

- Background……Slides 10-16

- Experimentation……Slides 17-28

- Conclusion……Slides 29-33

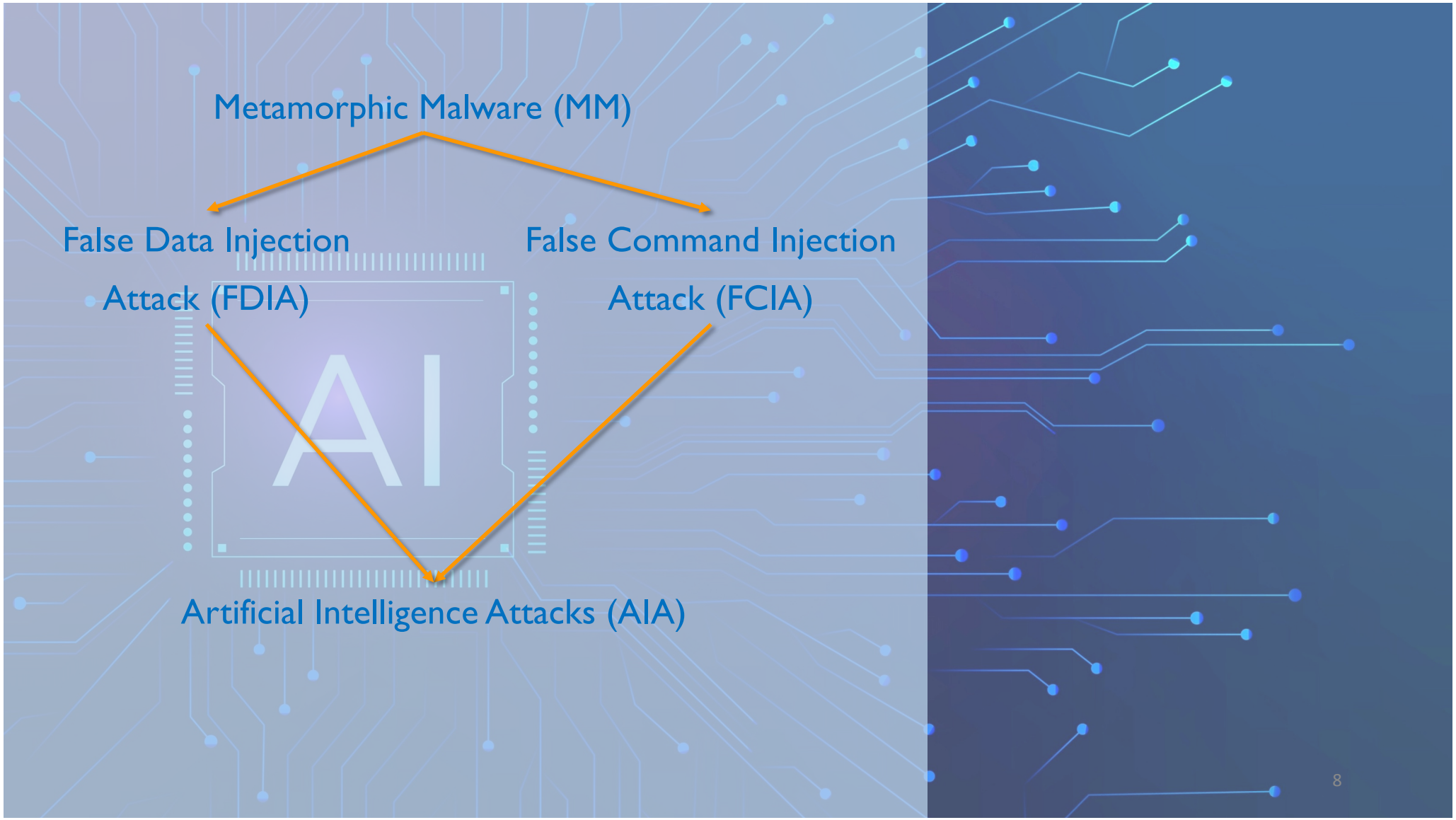
Introduction

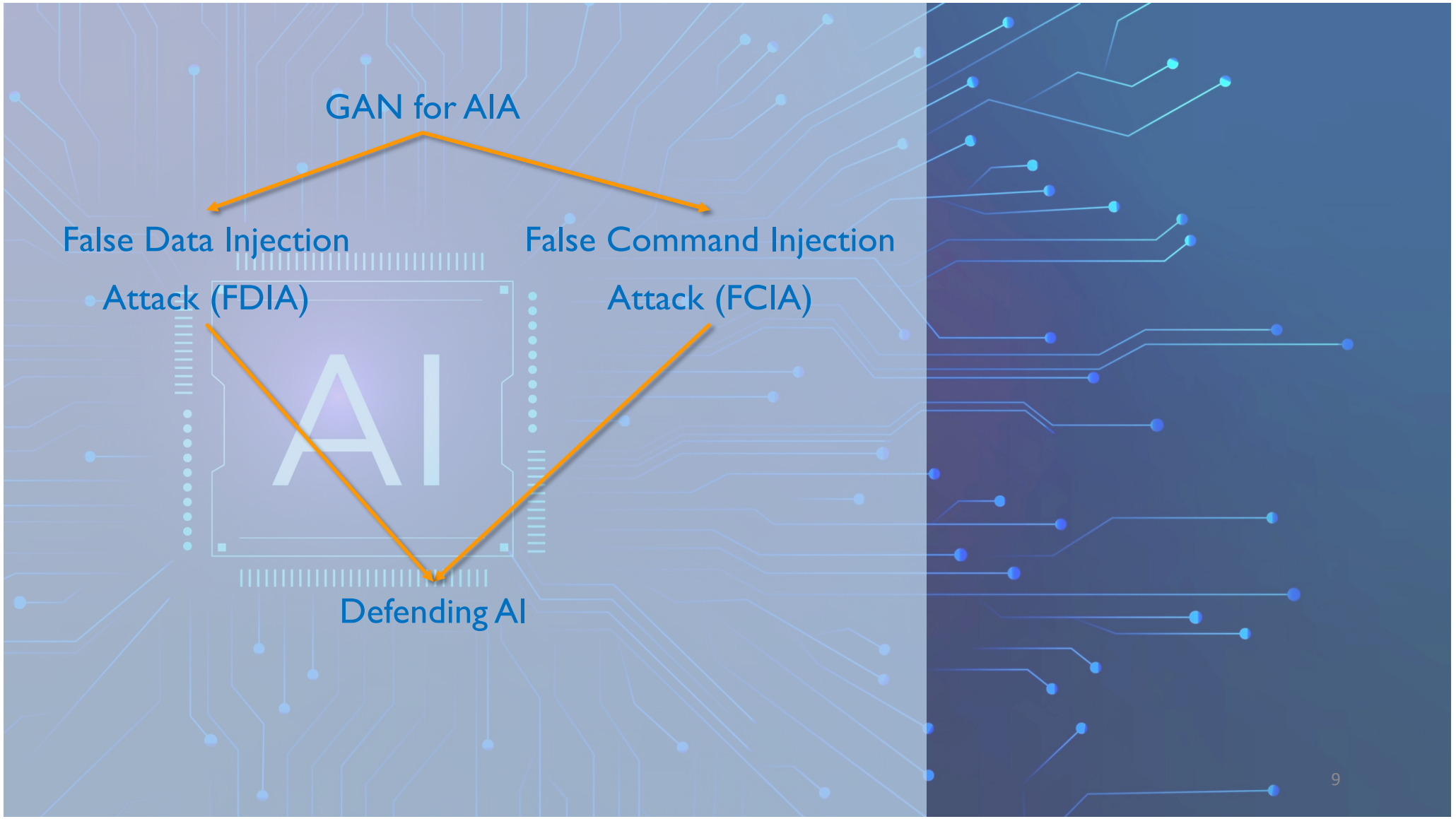
Builds upon the work from IARIA Cyber

1. Polymorphic Malware

2. Metamorphic Malware

3. Artificial Intelligence Attacks (AIA)


Metamorphic Malware (MM)
False Data Injection Attack (FDIA)
False Command Injection Attack (FCIA)
AI
Artificial Intelligence Attacks (AIA)

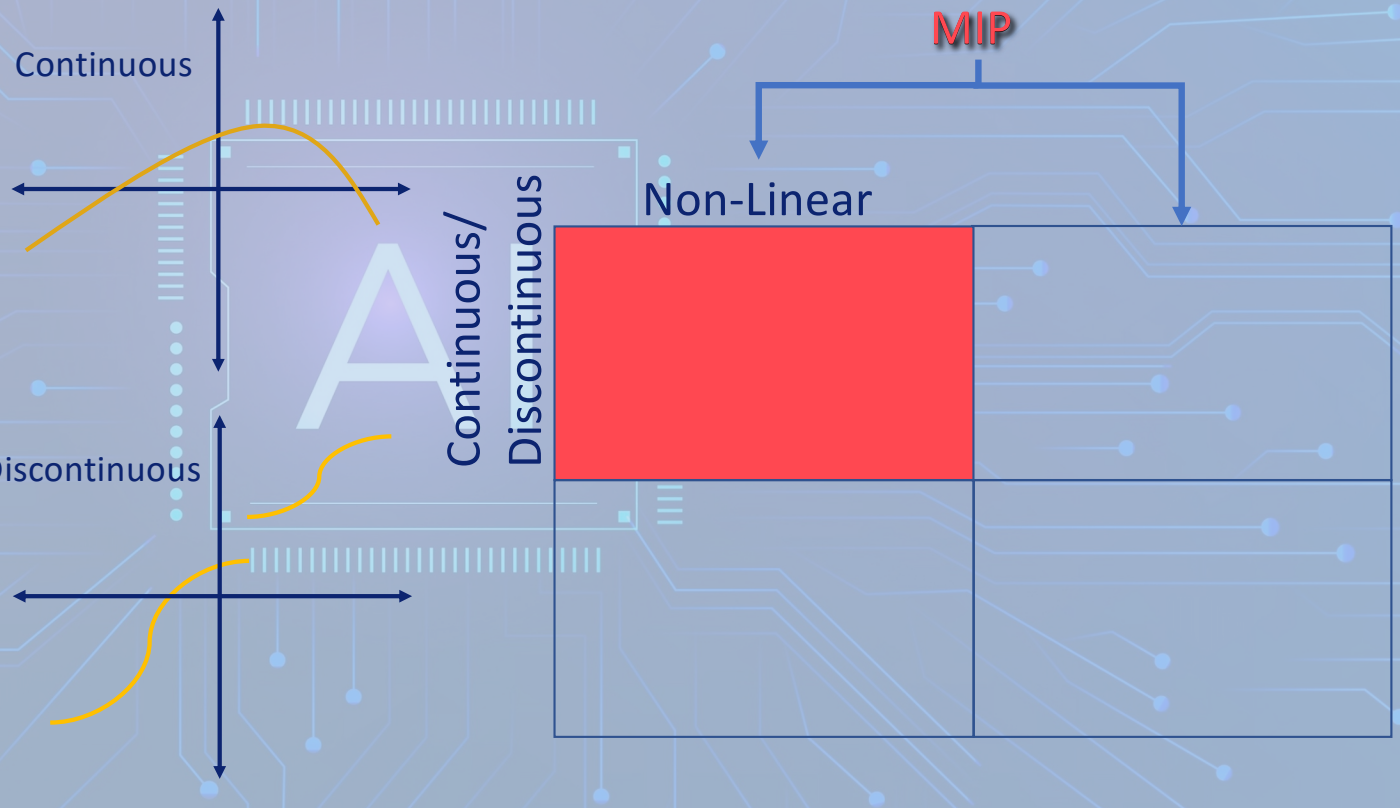

GAN for AIA
False Data Injection Attack (FDIA)
False Command Injection Attack (FCIA)
AI
Defending AI

Background

“Narrow Canyon Facilitation”

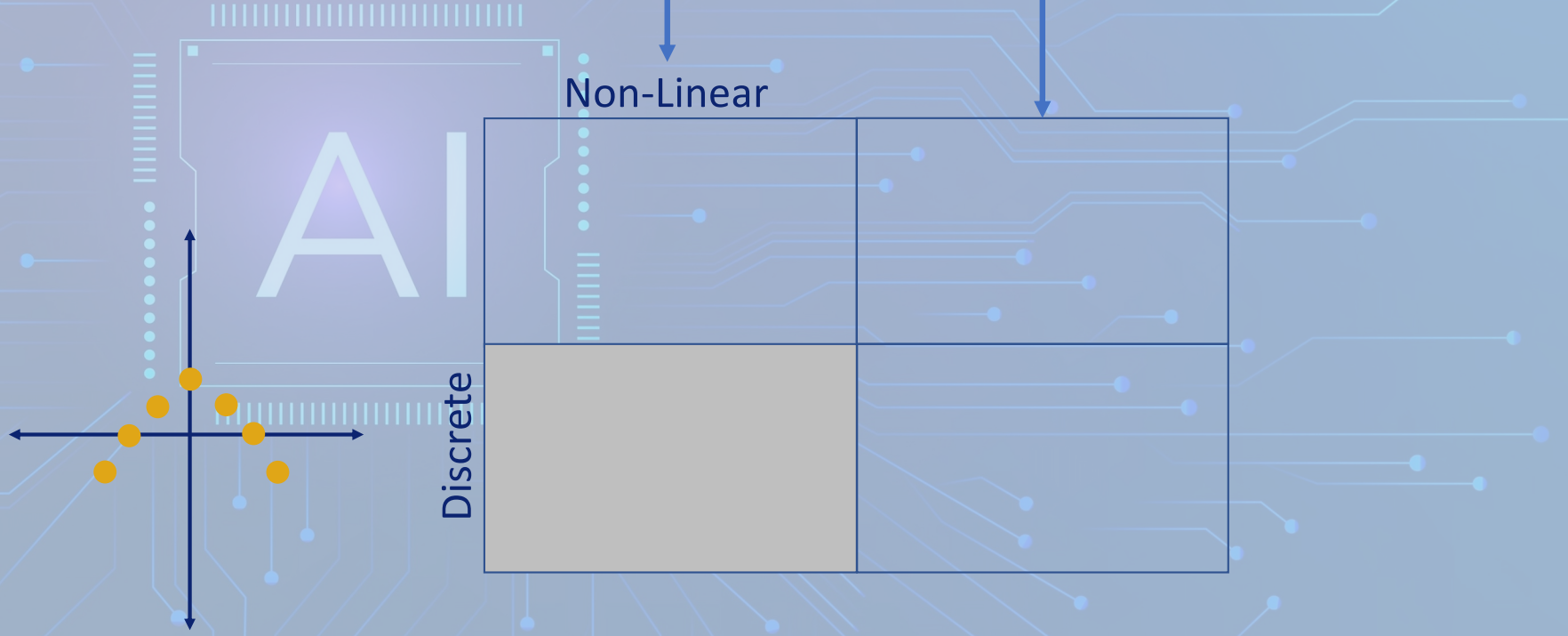
Mixed Integer Programming (MIP)

Non-Linear, Continuous/Discontinuous



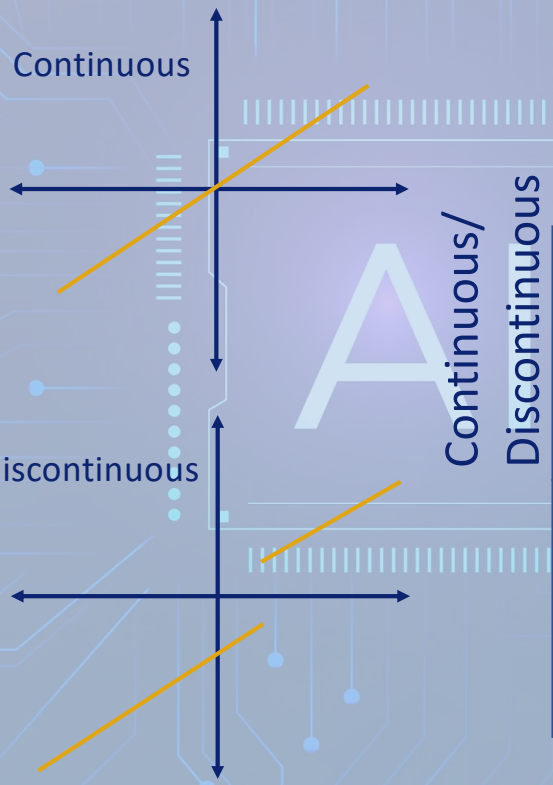
MIP PROBLEMS

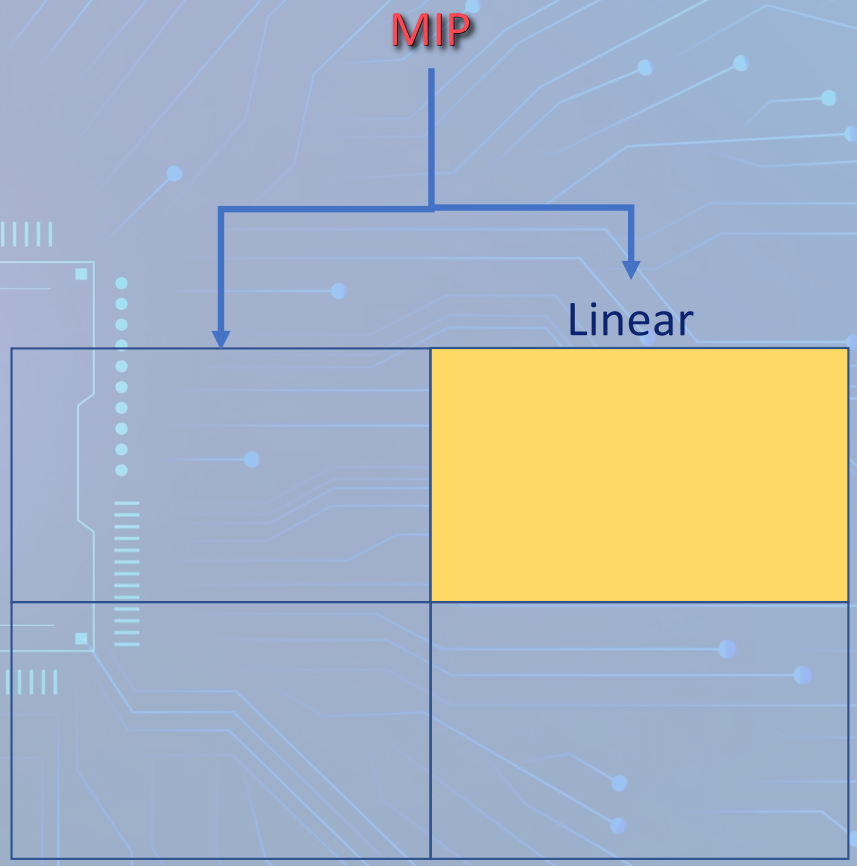
Non-Linear, Discrete



MIP PROBLEMS

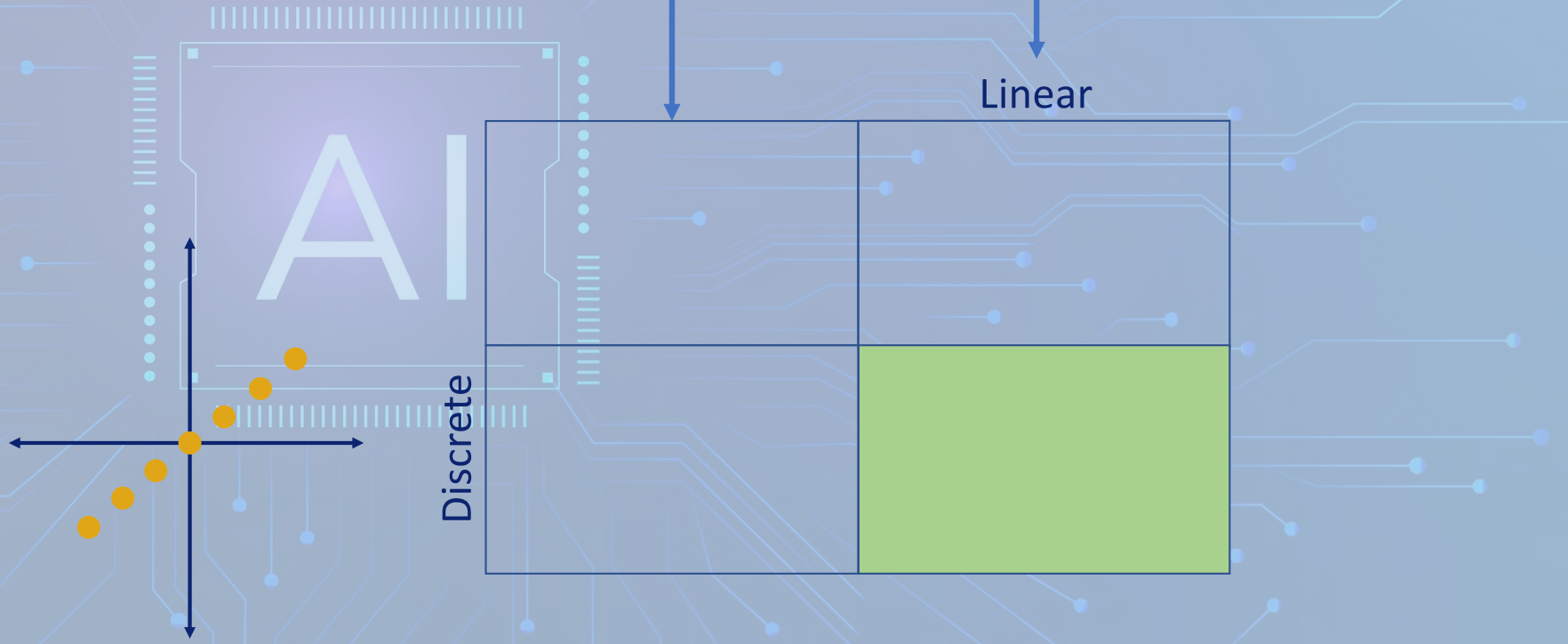
Linear, Continuous/Discontinuous





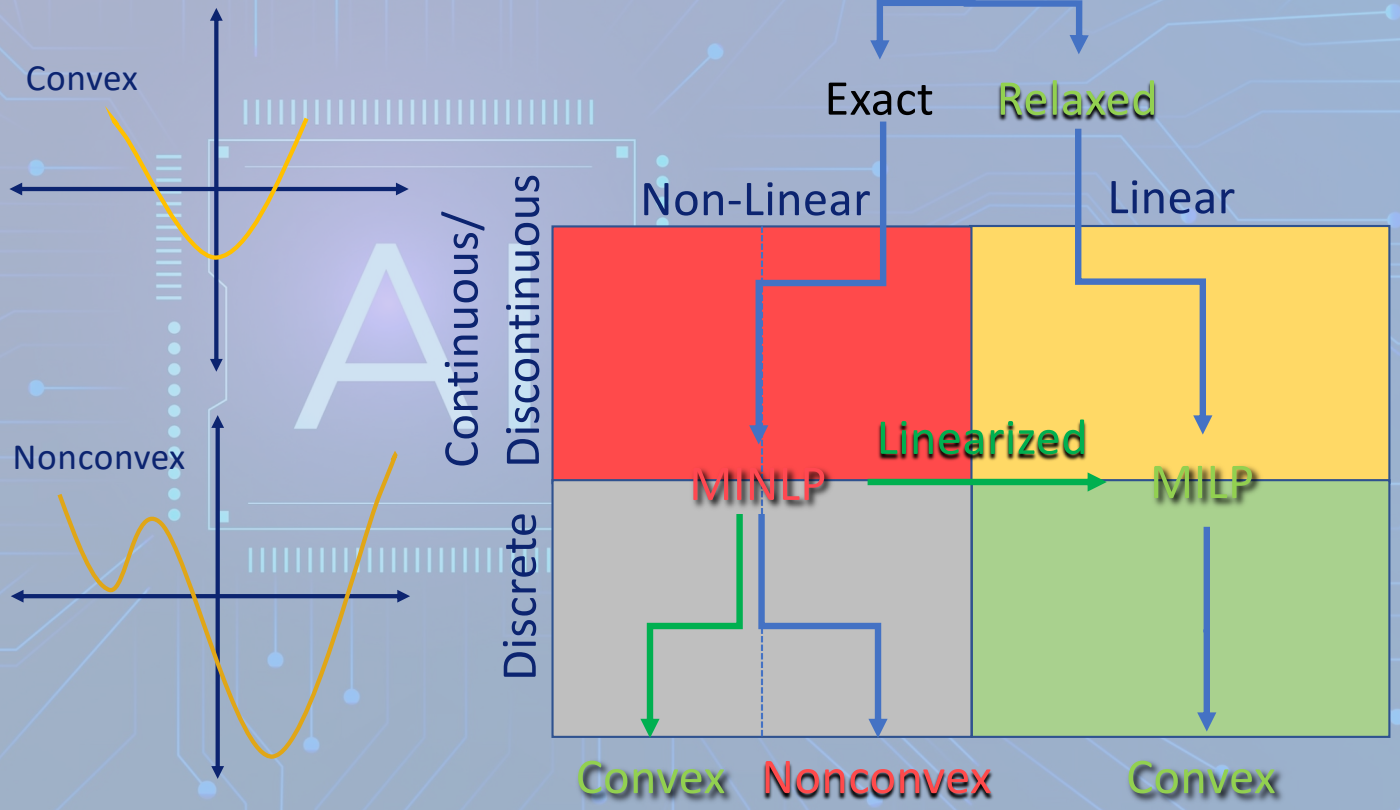
MIP PROBLEMS

Linear, Discrete



NONCONVEX PARADIGM

Mixed Integer Non-Linear Programming (MINLP) Problems

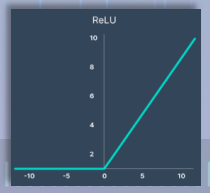


Experimentation

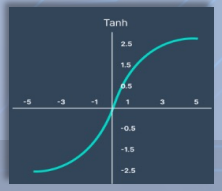
1. Diverse hybridized Activation Functions (AFs)

Rectified Linear Unit (ReLU)

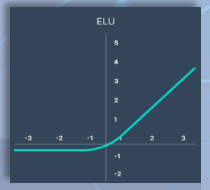
Highly Vulnerable to AIA



Tangent and Hyperbolic (Tanh)



Exponential Linear Unit (ELU)



AFs = Activation Functions

- Swish ← ReLU + Sigmoid
- Mish ← ReLU + Tanh + Softplus (e.g., a smooth ReLU)
- SCL Mish ← ReLU + Tanh + Softplus, wherein *α* is learnable
- ELU Mish ← ELU + Tanh + Softplus

SCL = Soft Clipping

ReLU -> Dying ReLU Problem – simply no activation

Sigmoid, Tanh -> Vanishing Gradient Problem

2. Bespoke Nonlinear Conjugate Gradient (NCG)/ Nesteror Accelerated Gradient (NAG) for Adaptive Momentum (ADaM)

Nonlinear Conjugate Gradient (NCG)

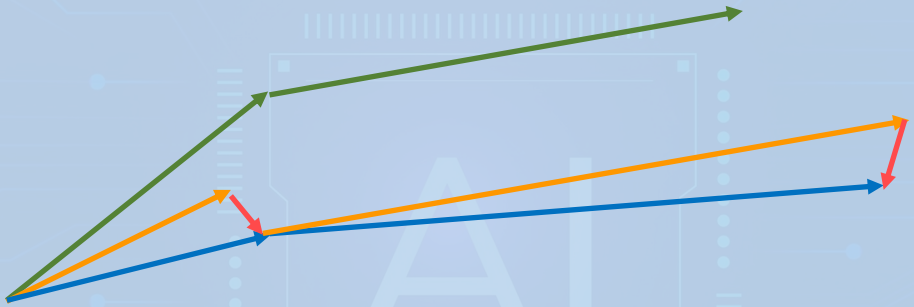
Best Initial Posit

Worst Initial Posit

NCG Posit

NCG -> widely used for unconstrained optimization

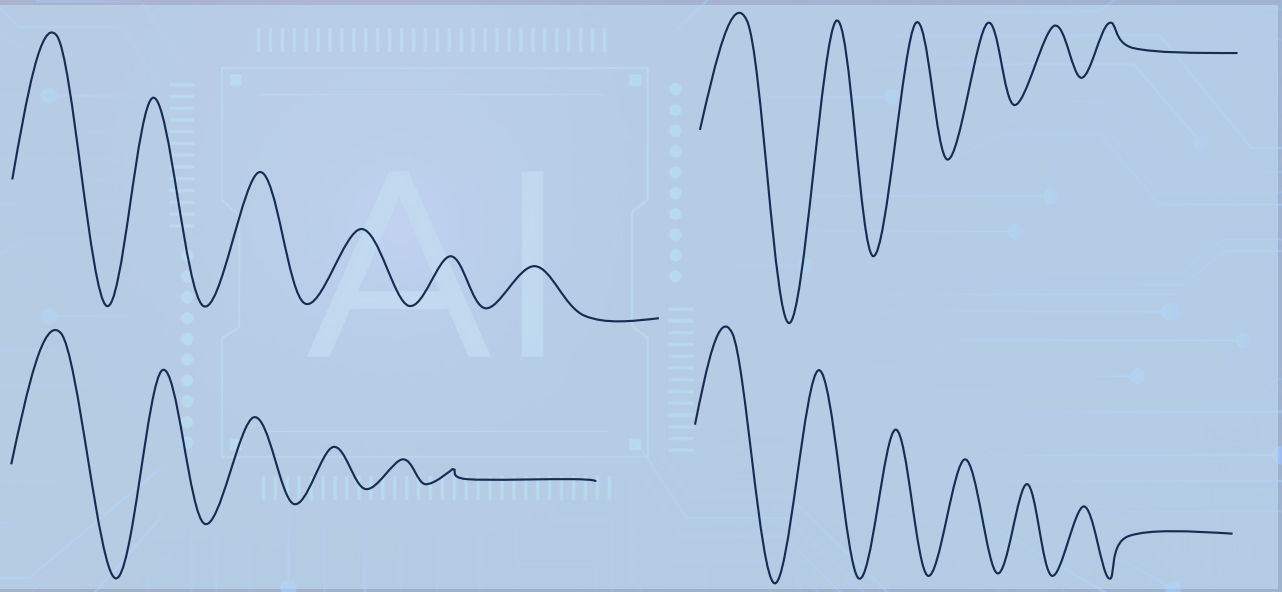
Nesterov Accelerated Gradient (NAG)



- Standard Momentum
- Accumulated Gradient
- NAG Posit/Jump
- Correction

NAG -> widely acknowledged as having better complexity bounds than NCG

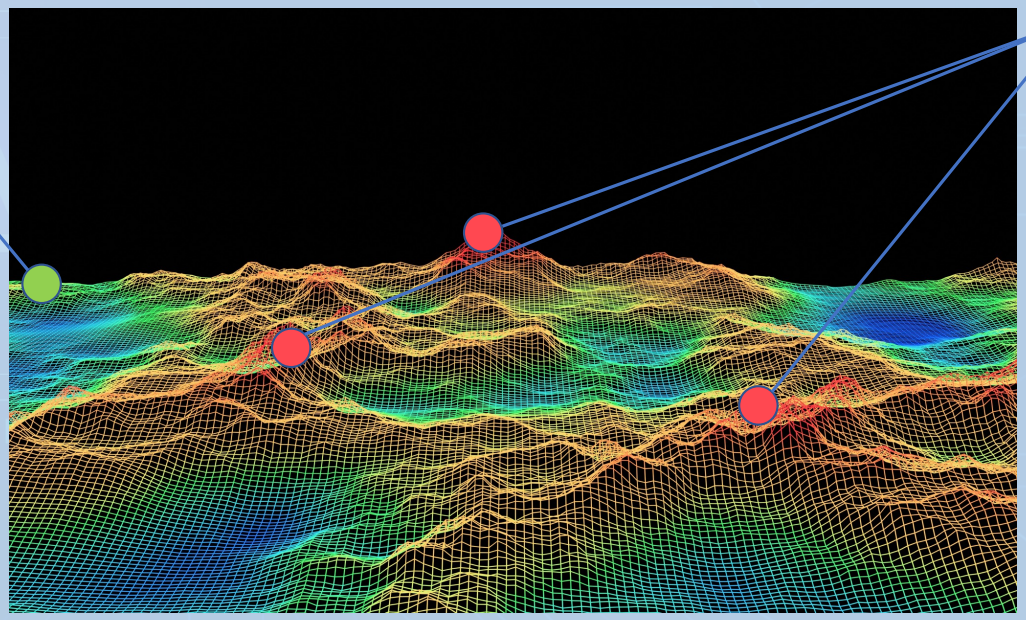
ADaptive Momentum (ADaM) Oscillation Dampener



ADaptive Momentum (ADam) as an additional parameter of an Adaptive Inertial Weighting System (AIW)

Instantiated atop a Modified GNU Octave (M-GNU-Octave) System

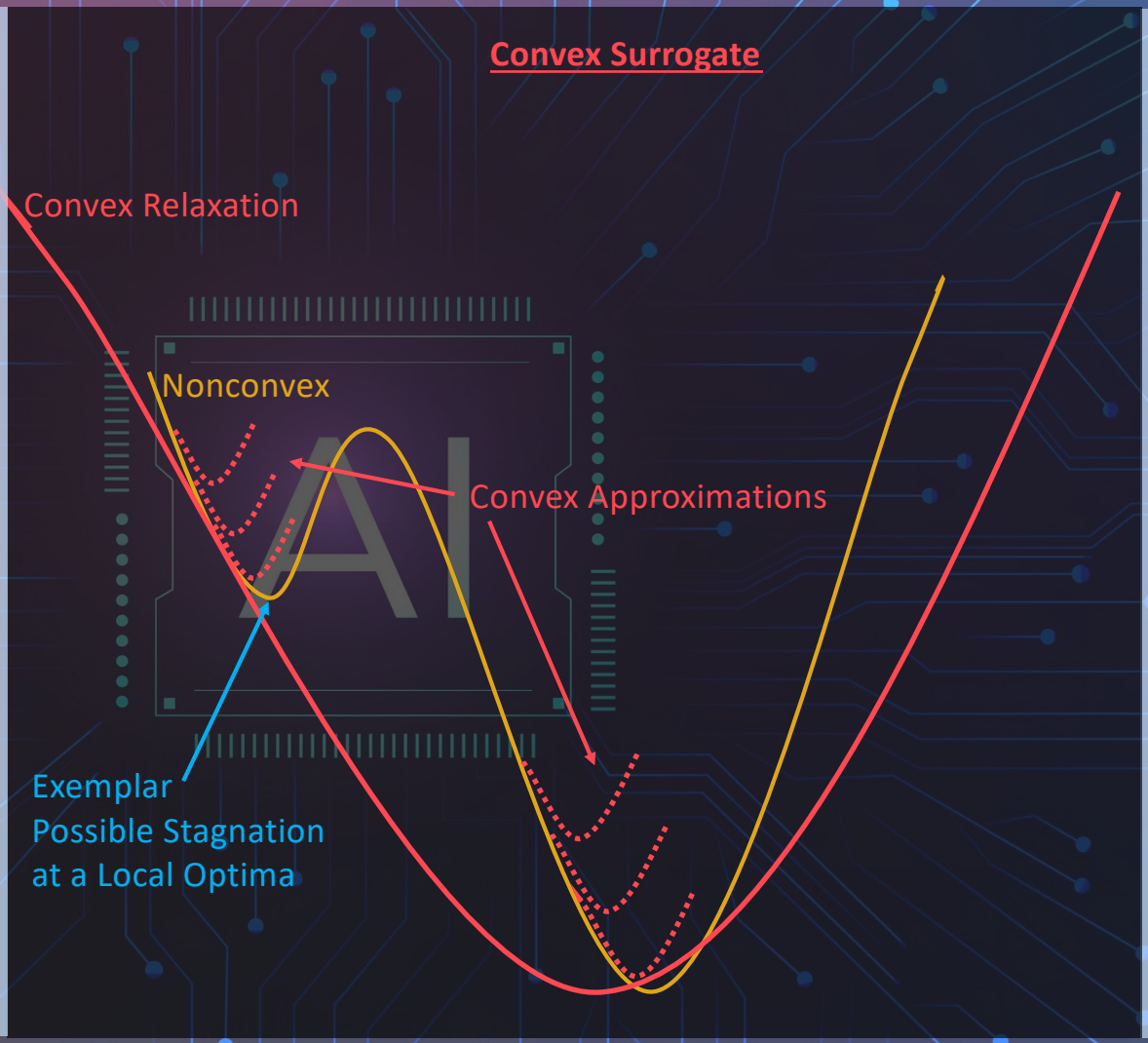
Global optimum



Mitigation of premature stagnation of the involved particles at local optima, via AIW.

Just enough;
Don't want to overshoot
The global optimum

3. Second-Order Cone Programming Relaxations (SOCPR) for Entropic Wavelet Energy Spectrum (EWES) Discernment (ED)



Conventional Challenge:

- Requires converting continuous/discontinuous hyperparameters to discrete values, which can lead to premature stagnation of particles at local optima

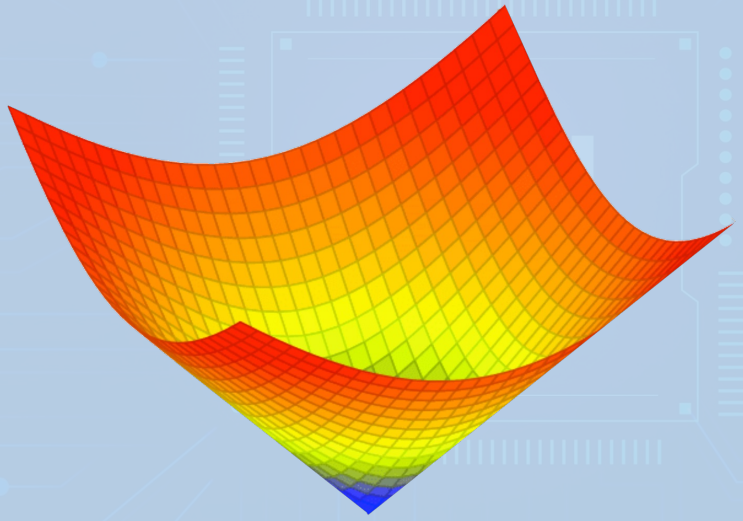
Our Utilized Approach:

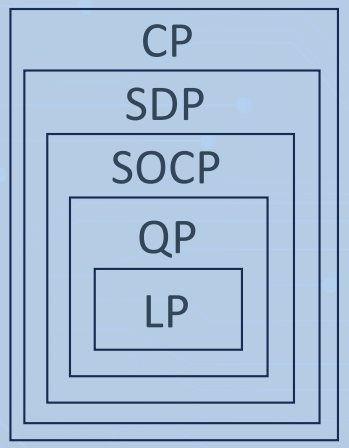
- Convex Surrogates, Approximation, Series of Robust Convex Relaxations (RCR)

The Promise of PSO-based RCR

- Facilitates valid bounds for near-optimal convex optimization solutions
- Reduced number of hyperparameters to tune, via a specific implementation of the bespoke architectural construct.
- Increasing the inertial weighting may spawn further nonconvex problems; however, the RCR approach has high efficacy.

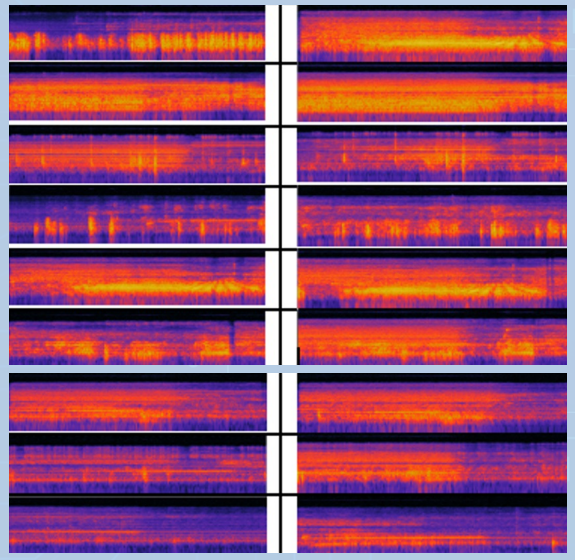
Second-Order Cone Programming Relaxations

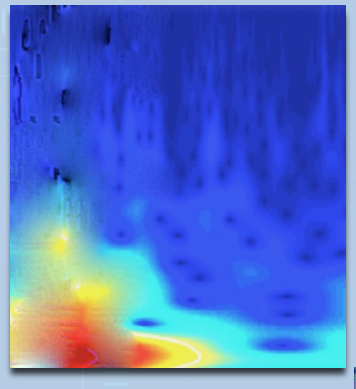


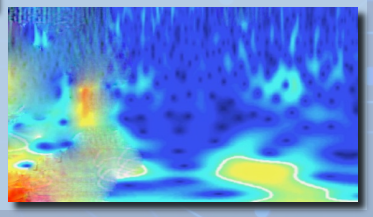


LP = Linear Programming; QP = Quadratic Programming; SOCP = Second-Order Cone Programming; SDP = Semidefinite Programming; CP = Cone Programming

Entropic Wavelet Energy Spectrum (EWES) Discernment (ED)







Conclusion

Higher Efficacy Detection of Artificial Intelligence Attacks (AIA)

1. Hybridized Activation Function (AF) ELU Mish

+

2. Bespoke Nonlinear Conjugate Gradient (NCG)/

Nesteror Accelerated Gradient (NAG)

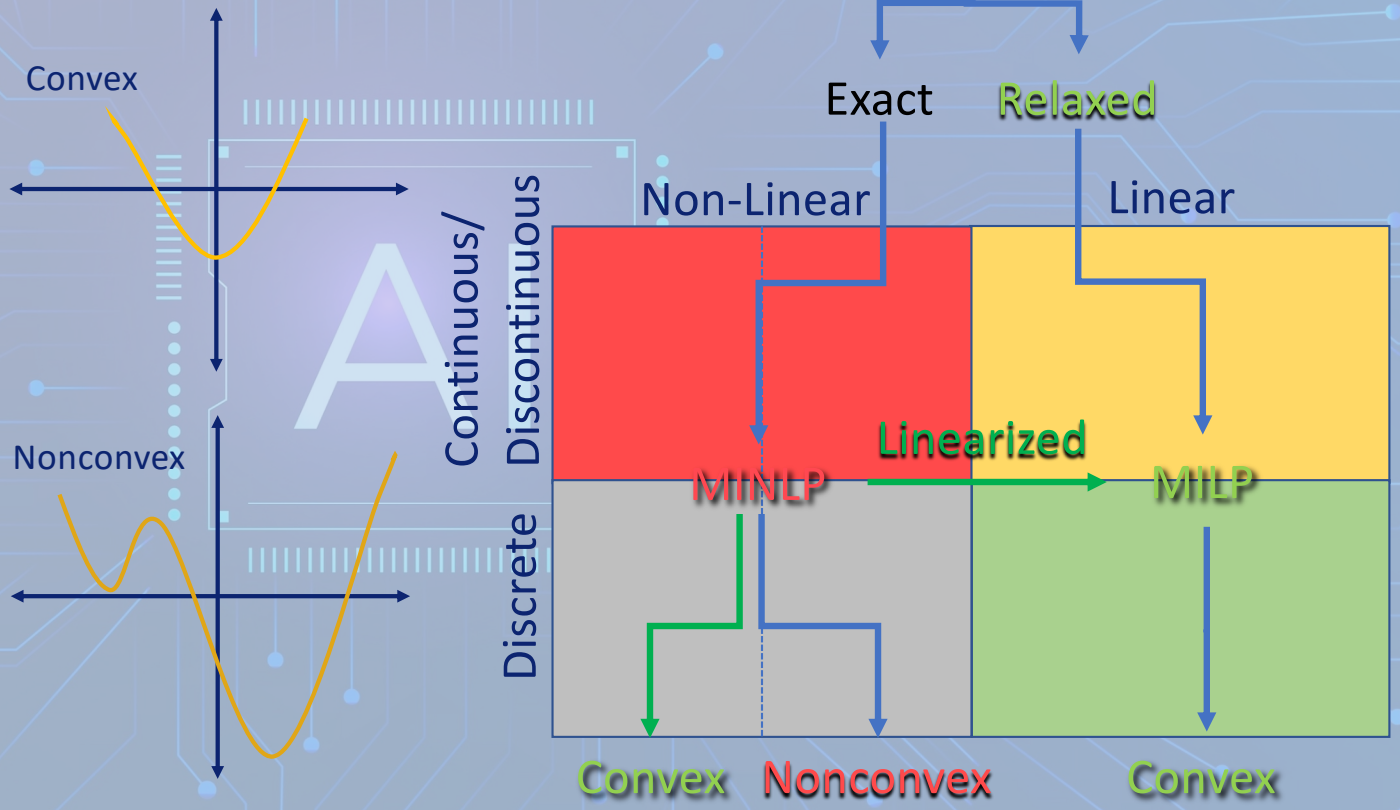
for Adaptive Momentum (ADaM) for an enhanced AIW

+

3. Second-Order Cone Programming Relaxations (SOCPR) for Entropic Wavelet Energy Spectrum (EWES) Discernment (ED) for a particular Suspiciously Structured Entropic Change Score (SSECS)

NONCONVEX PARADIGM

Mixed Integer Non-Linear Programming (MINLP) Problems



Ill-Conditioned Optimization Problems
(a.k.a., “Narrow Canyon Facilitation”)

The 2023 IARIA Annual Congress on Frontiers in Science, Technology, Services, and Applications (IARIA Congress 2023)

The Triumvirate of Bespoke Diverse Hybridized Activation Functions, Adaptive Momentum, and Enhanced Entropic Wavelet Energy Spectrum Discernment for Higher Efficacy Detection of Artificial Intelligence-centric Attacks

Thank You!

Steve Chan
schan@dengineering.org