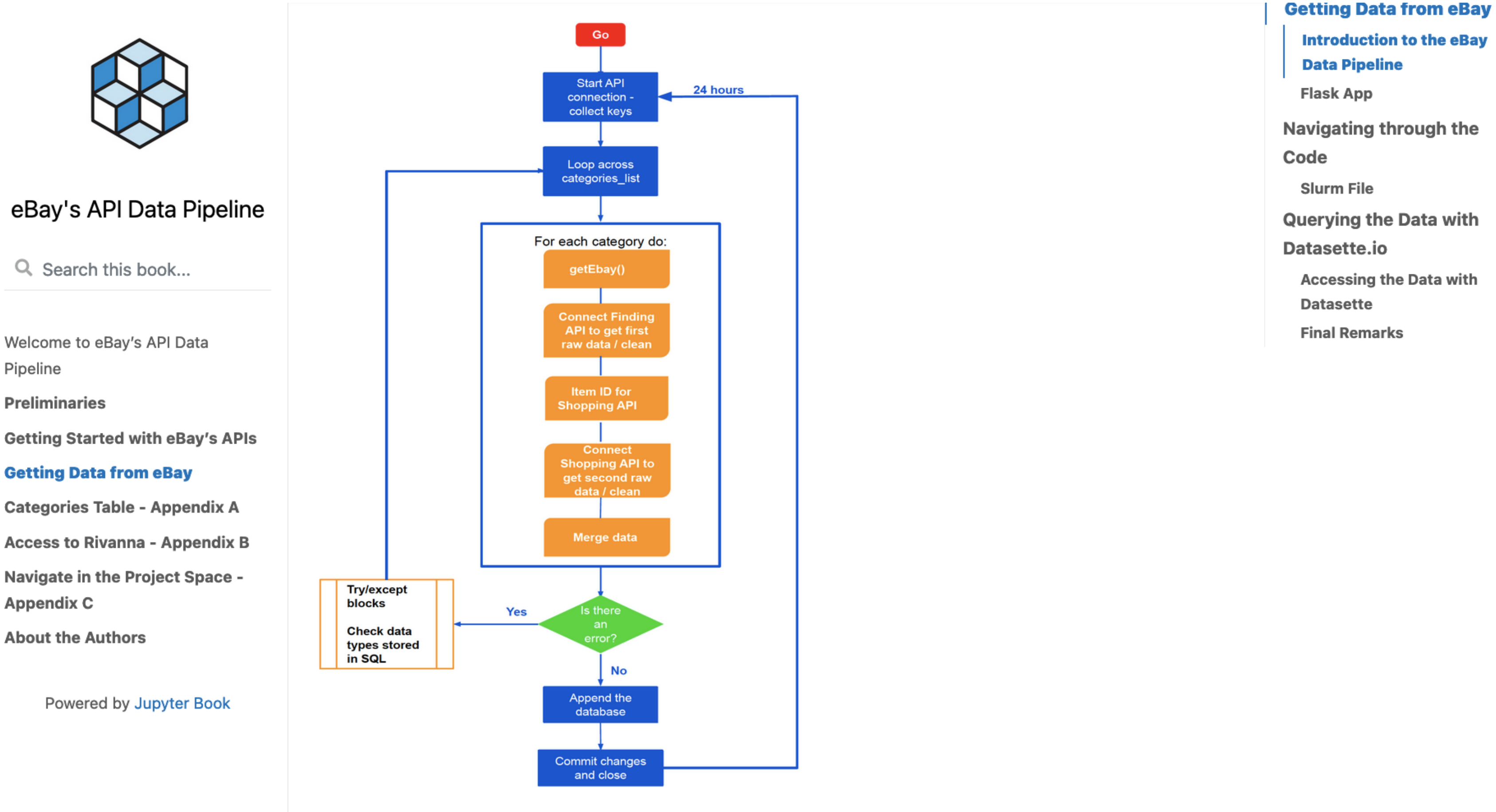
ML Systems: security & privacy

Joseph Choi, Karolina Naranjo

Dataset

- Medical imaging (Xray, CT, MRI)
- Cloud point data (human)
- Person in vehicle
- Materials data:
  (2D & 3D microstructure image)
- US supreme court data (SQLite)

Karolina’s previous research works



eBay's API Data Pipeline

Search this book...

Powered by Jupyter Book

Go

Start API connection - collect keys

24 hours

Loop across categories_list

For each category do:

getEbay()

Connect Finding API to get first raw data / clean

Item ID for Shopping API

Connect Shopping API to get second raw data / clean

Merge data

Is there an error?

Yes

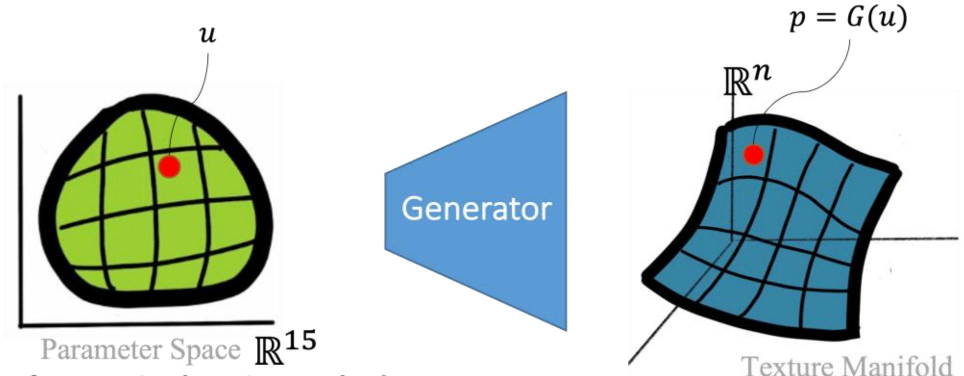
Try/except blocks

Check data types stored in SQL

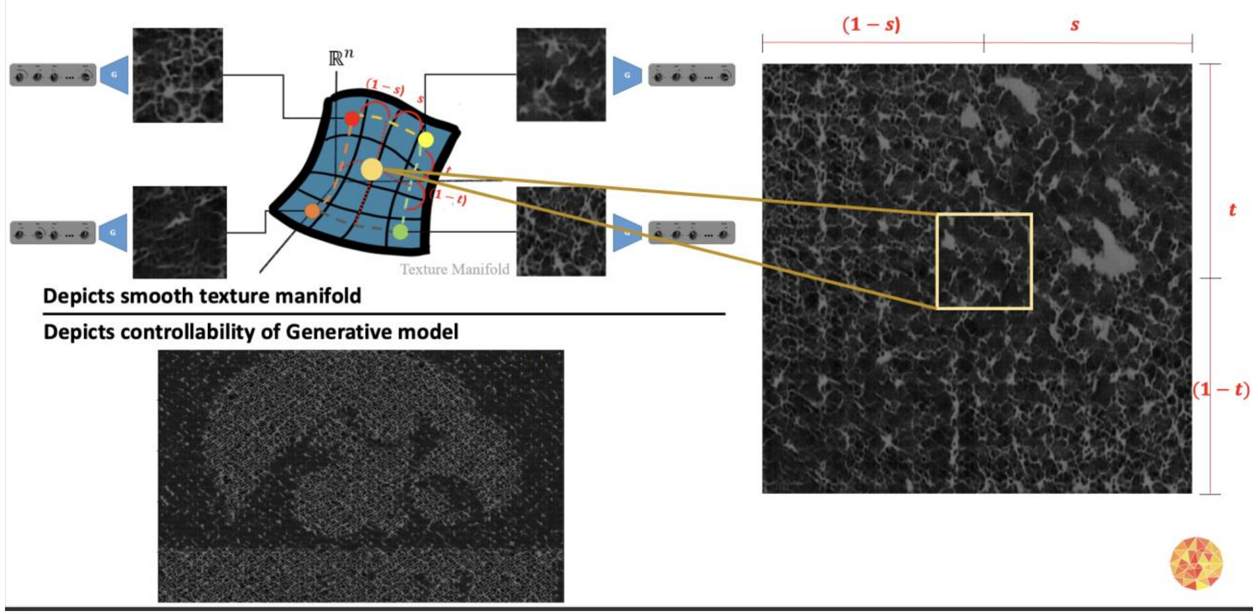
No

Append the database

Commit changes and close

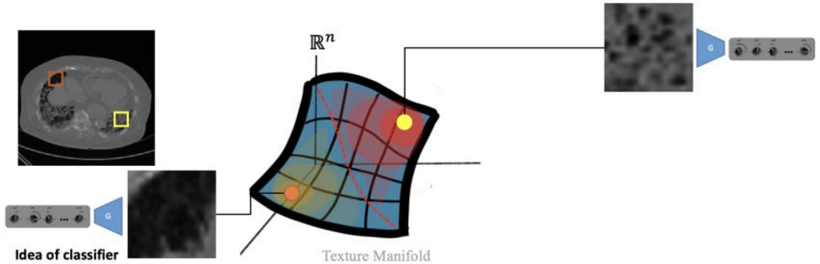


Idea of generative learning method

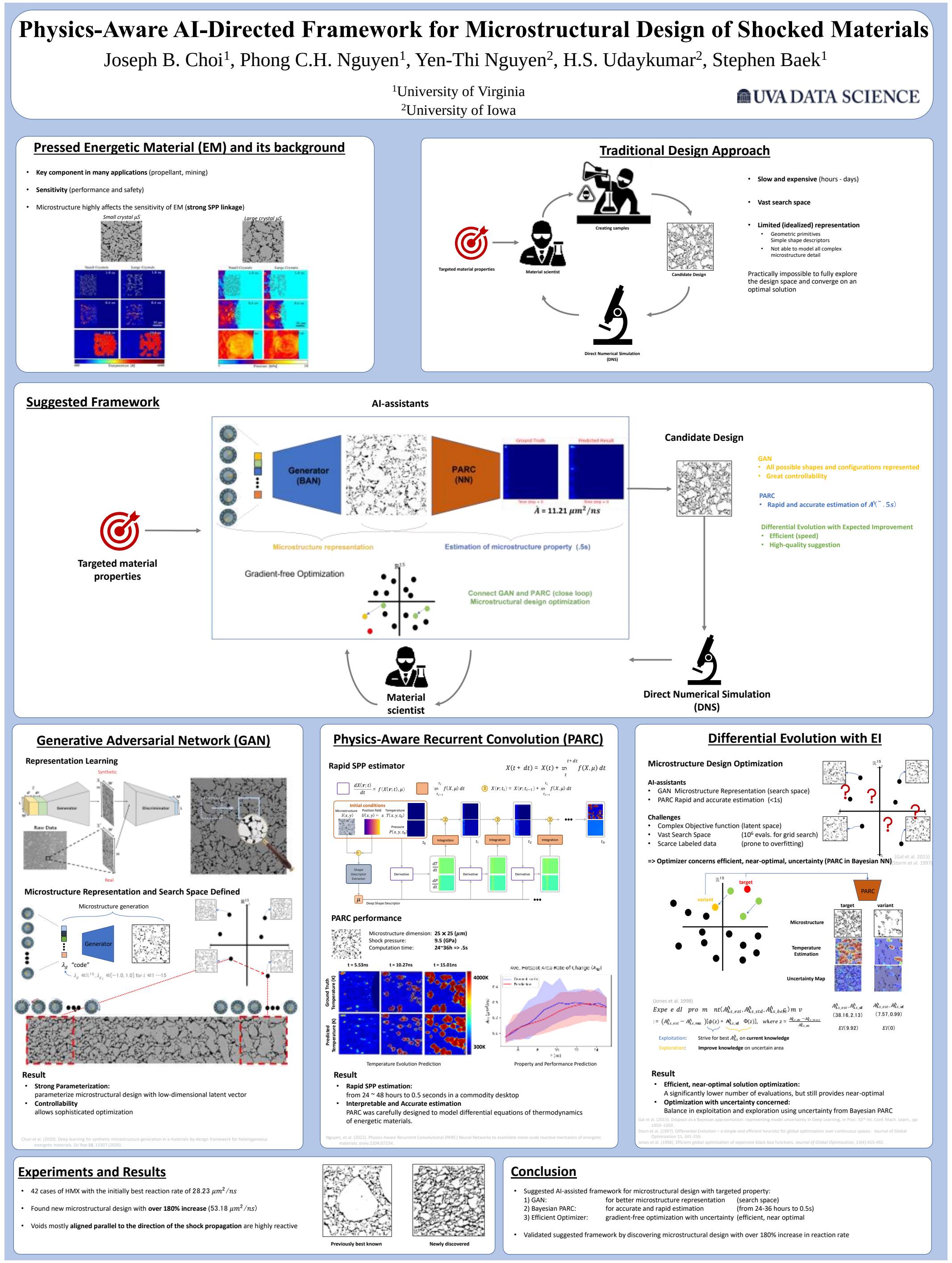


Depicts smooth texture manifold

Depicts controllability of Generative model



Idea of classifier



Physics-Aware AI-Directed Framework for Microstructural Design of Shocked Materials

Joseph B. Choi[1], Phong C.H. Nguyen[1], Yen-Thi Nguyen[2], H.S. Udaykumar[2], Stephen Baek[1]

[1]University of Virginia
[2]University of Iowa

UVA DATA SCIENCE

Pressed Energetic Material (EM) and its background

- **Key component in many applications** (propellant, mining)
- **Sensitivity** (performance and safety)
- Microstructure highly affects the sensitivity of EM (**strong SPP linkage**)

Small crystal μS *Large crystal μS*

Traditional Design Approach

Targeted material properties → Material scientist → Creating samples → Candidate Design → Direct Numerical Simulation (DNS)

- **Slow and expensive** (hours - days)
- **Vast search space**
- **Limited (idealized) representation**
  - Geometric primitives
    Simple shape descriptors
  - Not able to model all complex microstructure detail

Practically impossible to fully explore the design space and converge on an optimal solution

Suggested Framework

AI-assistants

Generator (BAN) → PARC (NN) → Ground Truth / Predicted Result

$\dot{A} = 11.21\ \mu m^2/ns$

Microstructure representation

Estimation of microstructure property (.5s)

Gradient-free Optimization

Connect GAN and PARC (close loop)
Microstructural design optimization

Targeted material properties

Candidate Design

Material scientist

Direct Numerical Simulation (DNS)

GAN
- All possible shapes and configurations represented
- Great controllability

PARC
- Rapid and accurate estimation of $\dot{A}$(~ .5s)

Differential Evolution with Expected Improvement
- Efficient (speed)
- High-quality suggestion

Generative Adversarial Network (GAN)

Representation Learning

Synthetic
Generator
Discriminator
Raw Data
Real

Microstructure Representation and Search Space Defined

Microstructure generation
Generator
λ_g "code"
$\lambda_g \in \mathbb{R}^{15}, \lambda_{g_i} \in [-1.0, 1.0]$ for $i \in 1 \cdots 15$

Result

- **Strong Parameterization:**
  parameterize microstructural design with low-dimensional latent vector
- **Controllability**
  allows sophisticated optimization

Chun et al. (2020). Deep learning for synthetic microstructure generation in a materials-by-design framework for heterogeneous energetic materials. *Sci Rep* **10**, 13307 (2020).

Physics-Aware Recurrent Convolution (PARC)

Rapid SPP estimator

$X(t+dt) = X(t) + \int_t^{t+dt} f(X,\mu)\,dt$

$\frac{dX(\mathbf{r};t)}{dt} = f(X(\mathbf{r};t),\mu)$ $\int_{t_{i-1}}^{t_i} f(X,\mu)\,dt$ $X(\mathbf{r};t_i) = X(\mathbf{r};t_{i-1}) + \int_{t_{i-1}}^{t_i} f(X,\mu)\,dt$

Initial conditions: Microstructure $I(x,y)$, Position field $U(x,y) = x$, Temperature $T(x,y,t_0)$, Pressure $P(x,y,t_0)$

Shape Descriptor Extractor → μ Deep Shape Descriptor → Derivative → $\frac{dT}{dt}$, $\frac{dP}{dt}$ → Integration → $t_0, t_1, t_2, \ldots, t_N$

PARC performance

Microstructure dimension: **25 × 25 (μm)**
Shock pressure: **9.5 (GPa)**
Computation time: **24~36h => .5s**

t = 5.53ns t = 10.27ns t = 15.01ns
Ground Truth Temperature (K)
Predicted Temperature (K)
4000K
300K
Ave. Hotspot Area Rate of Change ($\dot{a}_{hs}$)

Temperature Evolution Prediction

Property and Performance Prediction

Result

- **Rapid SPP estimation:**
  from 24 ~ 48 hours to 0.5 seconds in a commodity desktop
- **Interpretable and Accurate estimation**
  PARC was carefully designed to model differential equations of thermodynamics of energetic materials.

Nguyen, et al. (2022). Physics-Aware Recurrent Convolutional (PARC) Neural Networks to assimilate meso-scale reactive mechanics of energetic materials. *arxiv:2204:07234.*

Differential Evolution with EI

Microstructure Design Optimization

AI-assistants
- GAN Microstructure Representation (search space)
- PARC Rapid and accurate estimation (<1s)

Challenges
- Complex Objective function (latent space)
- Vast Search Space (10⁶ evals. for grid search)
- Scarce Labeled data (prone to overfitting)

=> Optimizer concerns efficient, near-optimal, uncertainty (PARC in Bayesian NN) (Gal et al. 2015) (Storm et al. 1997)

$\mathbb{R}^{15}$ target variant PARC

	target	variant
Microstructure		
Temperature Estimation		
Uncertainty Map		
	$\hat{A}_{hs\_est}, \hat{A}_{hs\_std}$ (38.16, 2.13) $EI(9.92)$	$\hat{A}_{hs\_est}, \hat{A}_{hs\_std}$ (7.57, 0.99) $EI(0)$

(Jones et al. 1998)

$Expe\ e\ dI\ \ pro\ \ m\ \ \ nt(\hat{A}_{hs\_est}, \hat{A}_{hs\_std}, \hat{A}_{hs\_best})\ m\ v$

$:= (\hat{A}_{hs\_est} - \hat{A}_{hs\_max})[\phi(z) + \hat{A}_{hs\_std}\ \Phi(z)],\ where\ z = \frac{\hat{A}_{hs\_est} - \hat{A}_{hs\_max}}{\hat{A}_{hs\_std}}$

Exploitation: Strive for best $\hat{A}_{hs}$ on **current knowledge**

Exploration: **Improve knowledge** on uncertain area

Result

- **Efficient, near-optimal solution optimization:**
  A significantly lower number of evaluations, but still provides near-optimal
- **Optimization with uncertainty concerned:**
  Balance in exploitation and exploration using uncertainty from Bayesian PARC

Gal et al. (2015). Dropout as a Bayesian approximation: representing model uncertainty in Deep Learning, In Proc. 33rd Int. Conf. Mach. Learn., pp. 1050–1059.
Storn et al. (1997). Differential Evolution – a simple and efficient heuristic for global optimization over continuous spaces. Journal of Global Optimization 11, 341-359.
Jones et al. (1998). Efficient global optimization of expensive black-box functions. *Journal of Global Optimization*, 13(4):455-492.

Experiments and Results

- 42 cases of HMX with the initially best reaction rate of 28.23 $\mu m^2/ns$
- Found new microstructural design with **over 180% increase** (53.18 $\mu m^2/ns$)
- Voids mostly **aligned parallel to the direction of the shock propagation** are highly reactive

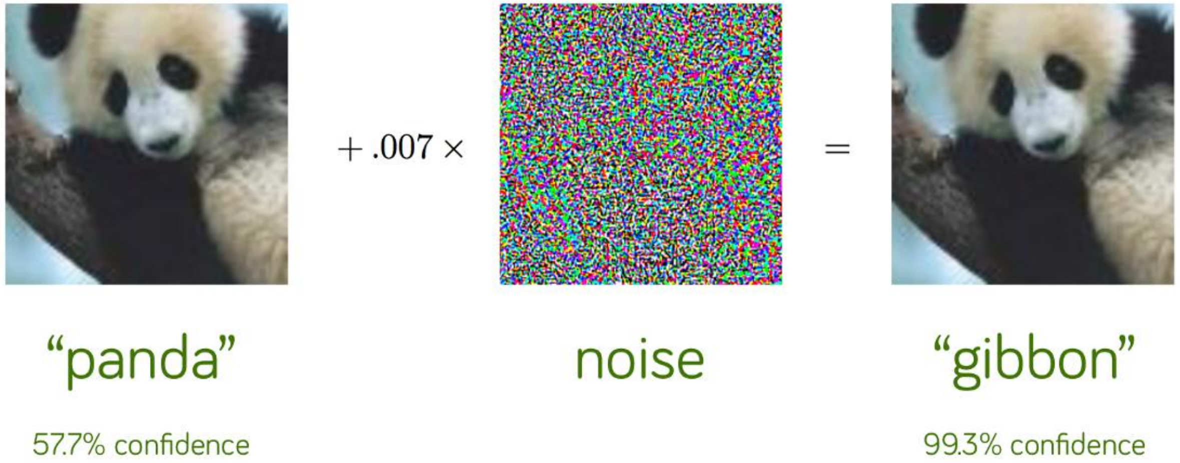
Previously best known **Newly discovered**

Conclusion

- Suggested AI-assisted framework for microstructural design with targeted property:
  1) GAN: for better microstructure representation (search space)
  2) Bayesian PARC: for accurate and rapid estimation (from 24-36 hours to 0.5s)
  3) Efficient Optimizer: gradient-free optimization with uncertainty (efficient, near optimal
- Validated suggested framework by discovering microstructural design with over 180% increase in reaction rate

Interests & potential problem

- How **security** is important in Law-DL models?
  - The integration of AI into Law firms: contracts [Forbes, LawBots, link]
- Adversarial attack **on graph data** [2, 3, 4, 6]
  - How law data is different from conventional structured graph data?
- SCOTUS data + NLP => similar case based on topic/issue



Future Plan

- Potential data set
  - Justice: benchmark dataset of the U.S. Supreme Court
- Research tasks:
  - Identify some relevant features of the law dataset
  - Investigate and modify adversarial attacks on graph
    - Adversarial attack on graph [2, 3, 4, 6]
    - Tune the attack specific to the nature of the law data
  - Study the defense mechanism for adversarial attacks on graph

References

- [1] Adversarial attack:
- Adversarial attach on the graph data:
  - [2] link,
  - [3] link
  - [4] link
- [5] LegalGNN
- Legal document classification, translation, summarization, contract review, case prediction and information retrieval
- [6] Review paper