QuantUniversity, LLC
www.quantuniversity.com

Qu Speaker Series

Machine Learning and Model Risk

(With a focus on Neural Networks)

An Afternoon with Dr. Agus Sudjianto

Wells Fargo

Hosted By:

Sri Krishnamurthy, CFA, CAP

sri@quantuniversity.com

www.qu.academy

07/29/2020

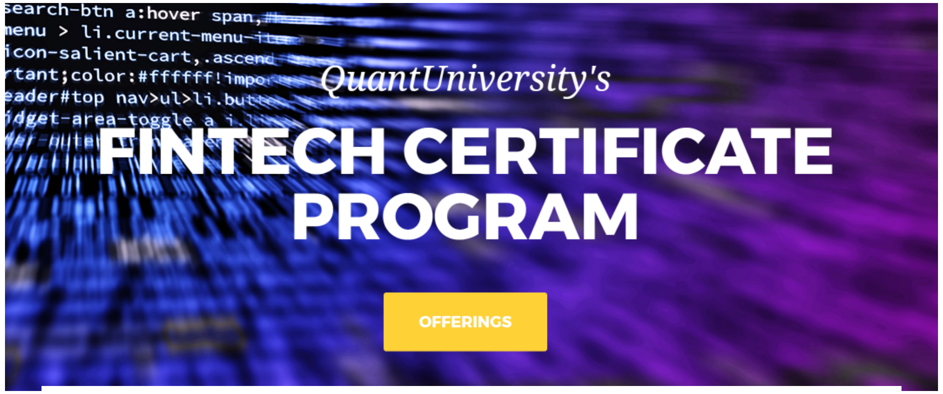
Online

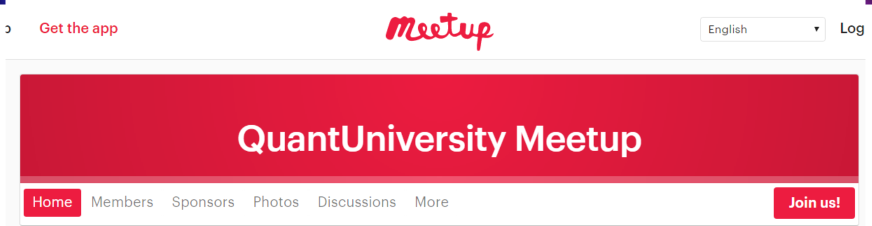
https://quspeakerseries3.splashthat.com/

2020 Copyright QuantUniversity LLC.

QuantUniversity

- Boston-based Data Science, Quant Finance and Machine Learning training and consulting advisory
- Trained more than 1000 students in Quantitative methods, Data Science and Big Data Technologies using MATLAB, Python and R
- Building QuSandbox a platform for AI and Machine Learning Exploration and Experimentation





QuantUniversity, LLC
www.quantuniversity.com

QuantUniversity Summer School 2020
www.qu.academy

QUANTUNIVERSITY
JUST ENOUGH PYTHON FOR DATA SCIENCE - FINANCE EDITION

Now Enrolling
Number of sessions: 3
Each session: 2.5 hours
Delivery: Online through QuAcademy with Video, Demos, Case studies + Labs

REGISTER

QUANTUNIVERSITY IN PARTNERSHIP WITH PRMIA PRESENTS

MACHINE LEARNING AND AI SUMMER SCHOOL FOR FINANCIAL PROFESSIONALS

Dates: July 9 - Sep 3rd 2020
Course duration: 1.5 hours/session - 9 weeks
Delivery: Online - through QuAcademy
Number of sessions: 9
Case studies + Labs using the QuSandbox

REGISTER

JUL 14TH, 11:00AM – AUG 25TH, 12:30PM
QUANTUNIVERSITY & PRMIA PRESENT:

MODEL RISK MANAGEMENT FOR MACHINE LEARNING MODELS

Model Risk Management for Machine Learning Models master class conducted in partnership with PRMIA

REGISTER

For registration information, go to
https://QuSummerSchool.splashthat.com

QU Speaker Series

Generating Synthetic Data with Generative Adversarial Networks (GANs)

Dr.Guilia Fanti
Carnegie Mellon University

https://quspeakerseries4.splashthat.com/

Wednesday, August 05 at 12:00pm

Dr.Guilia Fanti

Dr. Giulia Fanti is an Assistant Professor of Electrical and Computer Engineering at Carnegie Mellon University. Her research interests span the algorithmic foundations of blockchains, distributed systems, privacy-preserving technologies, and machine learning.

She is a fellow for the World Economic Forum's Global Future Council on Cybersecurity, and has received best paper awards from ACM Sigmetrics and ACM MobiHoc, as well as an NSF Graduate Research Fellowship.

Guilia is a recent recipient of the Faculty Research Award given by J.P.Morgan Chase on generating synthetic time series datasets

She obtained her Ph.D. in EECS from U.C. Berkeley and her B.S. in ECE from Olin College of Engineering.

QuantUniversity, LLC
www.quantuniversity.com

Schedule

12.00 - 12.05 PM	**Welcome Remarks - Sri Krishnamurthy, QuantUniversity**	Sri Krishnamurthy, QuantUniversity
12.05 - 12.40 PM	**Machine Learning and Model Risk (With a focus on Neural Network Models)**	Dr.Agus Sudjianto, Wells Fargo
12.40 - 1.00 PM	**Fireside Chat + Q&A**	

Dr.Agus Sudjianto, Wells Fargo

Dr.Agus Sudjianto is an executive vice president and head of Corporate Model Risk for Wells Fargo, where he is responsible for enterprise model risk management.

Prior to his current position, Agus was the modeling and analytics director and chief model risk officer at Lloyds Banking Group in the United Kingdom. Before joining Lloyds, he was a senior credit risk executive and head of Quantitative Risk at Bank of America.

Agus holds several U.S. patents in both finance and engineering. He has published numerous technical papers and is a co-author of Design and Modeling for Computer Experiments. His technical expertise and interests include quantitative risk, particularly credit risk modeling, machine learning and computational statistics.

He holds masters and doctorate degrees in engineering and management from Wayne State University and the Massachusetts Institute of Technology.

Sri Krishnamurthy, CFA

Sri Krishnamurthy, CFA is the Founder and CEO of QuantUniversity. Prior to that, Sri has worked at Citigroup, Endeca, MathWorks and with more than 25 customers in the financial services. Sri is the creator of QuSandbox, a platform for experimenting analytical and machine learning solutions for enterprises prior to adoption.

Sri teaches classes at QuAcademy (www.qu.academy) and teaches graduate courses in Machine Learning and AI at Northeastern University.

Sri earned an MS in Computer Systems Engineering and another MS in Computer Science, both from Northeastern University and an MBA from Babson College.

Machine Learning and Model Risk

- Dr.Agus Sudjianto is an executive vice president and head of Corporate Model Risk for Wells Fargo, where he is responsible for enterprise model risk management.

- Prior to his current position, Agus was the modeling and analytics director and chief model risk officer at Lloyds Banking Group in the United Kingdom. Before joining Lloyds, he was a senior credit risk executive and head of Quantitative Risk at Bank of America.

- Agus holds several U.S. patents in both finance and engineering. He has published numerous technical papers and is a co-author of Design and Modeling for Computer Experiments. His technical expertise and interests include quantitative risk, particularly credit risk modeling, machine learning and computational statistics.

- Agus holds masters and doctorate degrees in engineering and management from Wayne State University and the Massachusetts Institute of Technology.

Machine Learning Model Risk

(with special focus on machine learning explainability and robsustness)

July 29, 2020

Agus Sudjianto
EVP, Head of Enterprise Model Risk
Wells Fargo

© 2020 Wells Fargo Bank, N.A. All rights reserved. For public use.

Banks run by models

Banks pervasively use models

- Financial Models
  - Credit, Market, Liquidity, Revenue, Expense, Loss, Stress Test, Capital Management, Investment
- Non-Financial Models
  - Customer Service, Financial Crime Detection, Marketing, Compliance, Staffing

The use of model creates 'risk' both financial and non-financial risks and regulated throughout the life-cycle

- End-to-End model life cycle governance for all models
- Independent Model Validation
- Monitoring and Mitigation

https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf

Rapid adoption of ML in various areas of banking

Statistical models: Credit Risk and Financial Crimes

- Supervised and Unsupervised ML
- Alternative to more established statistical techniques
- Model benchmarks
- Model diagnostics and variable selection

Previously no models: Compliance, Conduct risk, Customer assistance

- Representation and Supervised/Unsupervised ML for Natural language processing

Intensive numerical computation: Derivative Pricing and Market Risk

- Deep Learning for stochastic PDE solver
- Generative Adversarial Network for stochastic process and time series models

https://arxiv.org/pdf/1807.06622.pdf
https://arxiv.org/pdf/1904.05921.pdf
https://arxiv.org/pdf/1911.12231.pdf
https://arxiv.org/pdf/2006.07635.pdf
https://arxiv.org/pdf/2005.10966.pdf

Model risk

All Models are **Wrong**
some are useful
- George Box

- Model error
- Used incorrectly

Model Failure: Potential *harms* and unintended consequences (to users, institution, or end customers) that a model may generate

- Financial harms (Credit, Market, Liquidity)
- Non-financial harms (Reputation, Compliance, Legal)

Example

- Hedging: mis-hedging $\rightarrow$ Market Risk
- Financial crimes or conduct surveillance: miss detection $\rightarrow$ Compliance risk
- Staffing: under staff (long wait time) $\rightarrow$ Reputational risk
- Credit approval: fair lending $\rightarrow$ Compliance risk
- On-line marketing: privacy and fairness $\rightarrow$ Legal risk

Model risk focus in model validation

Acceptance Metrics	Statistical (probabilistic) measure of harms and their acceptance criteria
Root Cause	‘Root causes’ analysis of harms/failure: data, input, modeling framework, variable selection, parameter estimation, implementation, misuse
Test to Failure	Robustness (adversarial) test to identify model failure
Impact Analysis	Quantify the impacts of each root cause
Mitigation Plan	Mitigation, monitoring and change control to manage potential harms

Common causes of ML model risk

Data defect and bias

- Input and target training data
- Beware of implicit bias

Conceptual Soundness

- Spurious variable effects due to confounding factors

Model robustness

- Obsession with model performance
- Dynamic real world: data drift

Model change control

- Retraining produces new models

Model use control

Conceptual soundness and explainable machine learning

Conceptual soundness and trusted model

- Does the model make sense? Can we trust the model? How’s the model going to fail?

Model explainability

- For critical applications, explainability is a requirement
  - Example: reason codes in credit decision is a regulatory requirement
- Outcome testing is not sufficient
  - Understanding Input-Output relationships are critical for Conceptual Soundness Evaluation
  - Confounding factors
  - Decision attribution and adverse impact
  - Failure operating region: output uncertainty and cautious generalization

Interpretable machine learning

Input-Output Explainability

Post-hoc analysis to understand input-output relationships

Model Distillation

Simplified and interpretable model

Structured-Interpretable Models

Interpretable model by constraining model structure

Post-hoc: Attribution through variable importance and effect

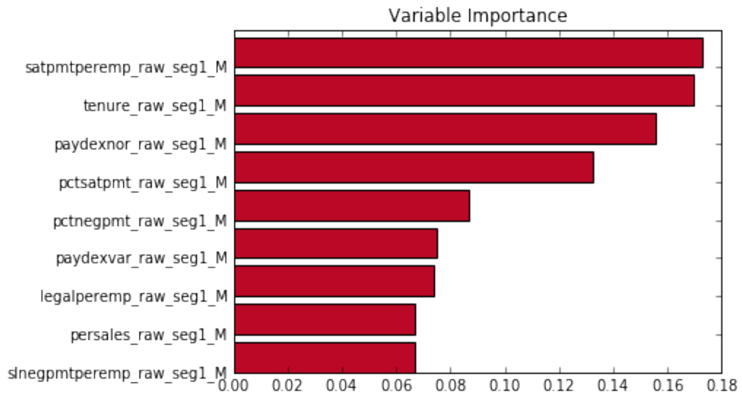
Global variable importance

- Relative influence
- Permutation test based importance
- Variance based global sensitivity (e.g., marginal effect and total effect)
- Derivative based sensitivity

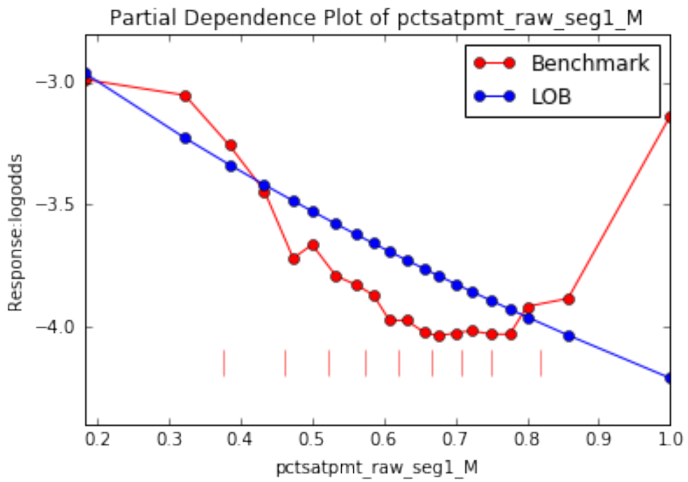
Local variable importance

- Leave-One-Covariate-Out (LOCO)
- Local sensitivity or partial derivative

- 1D partial dependent plots
  - Marginal effect
  - Nonlinearity detection
- 2D partial dependent plots and H statistics
  - Interaction effect

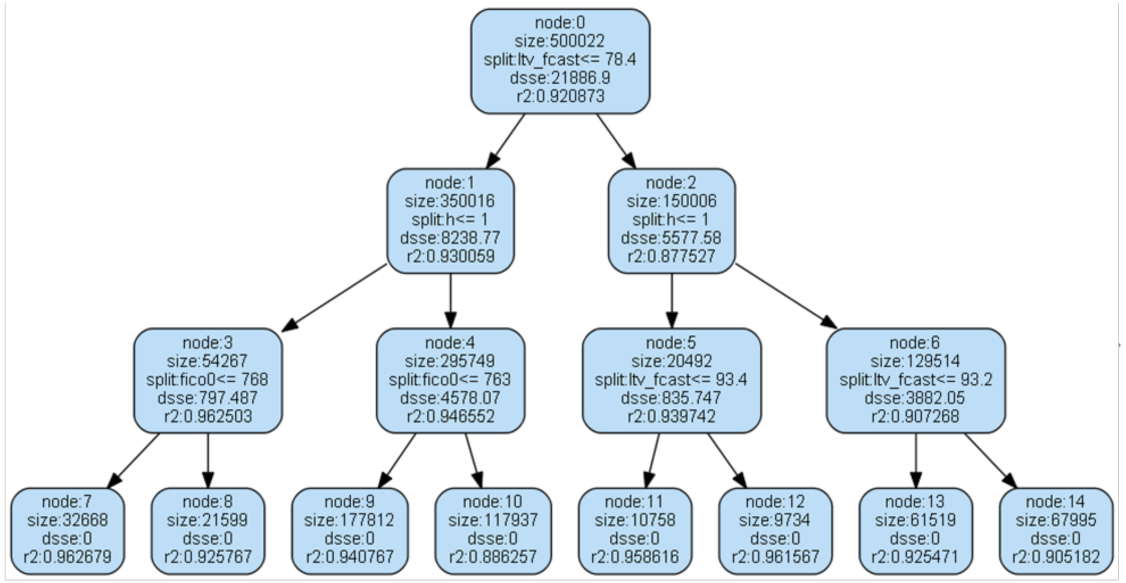


Feature transformation
Model Developers vs ML 1D-PDP



Model distillation

- Machine Learning Models, particularly ensemble models, are often too complex to be easily explained.
- Simplified—less accurate—models as ‘diagnostic’ tools
  - Meta/surrogate/emulator model also known as Model distillation



4	5	7	8	11	12	14	15
0.0014	0.0017	0.0036	0.0033	0.0244	0.0344	0.0255	0.0348
2	1.98	0.62	0.5	2.11	2.05	0.53	0.34
3.5	NA	2.12	2.95	3.09	4.01	1.53	2.26
-0.0105	-0.005	-0.0099	-0.0078	-0.0078	-0.0114	-0.007	-0.0117
0.06	0.073	0.06	0.076	0.043	0.071	0.043	0.072
-0.8	-0.35	-0.79	-0.4	-1.7	-0.69	-1.87	-0.83
-0.83	-0.35	-0.9	-0.43	-1.1	-0.7	-1.14	-0.75

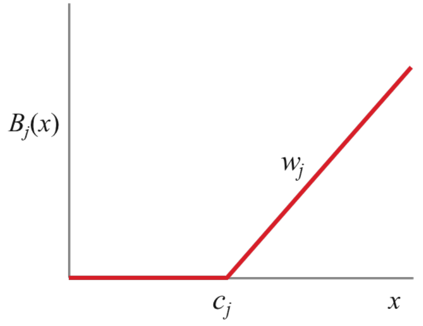
https://arxiv.org/ftp/arxiv/papers/1806/1806.00663.pdf

Interpretable model: Explainable neural networks (xNN)

Linear Model: $f(x) = w_0 + w\,x$

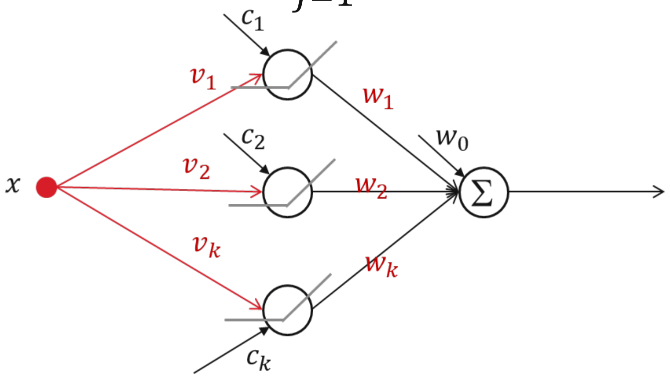
Nonlinear $f(x)$: Splines

$$f(x) = w_0 + \sum_{j=1}^{k} w_j\, B_j(x)$$



Nonlinear $f(x)$: Neural Networks

$$f(x) = w_0 + \sum_{j=1}^{k} w_j\, B_j\left(v_j\, x\right)$$



Single Index Model

$$f(\mathbf{x}) = w_0 + \sum_{j=1}^{k} w_j\, B_j\left(\mathbf{v}^{\mathrm{T}}\, \mathbf{x}\right)$$

Single Hidden Layer Network

$$f(\mathbf{x}) = w_0 + \sum_{j=1}^{k} w_j\, B_j\left(\mathbf{v}_j^{\mathrm{T}}\, \mathbf{x}\right)$$

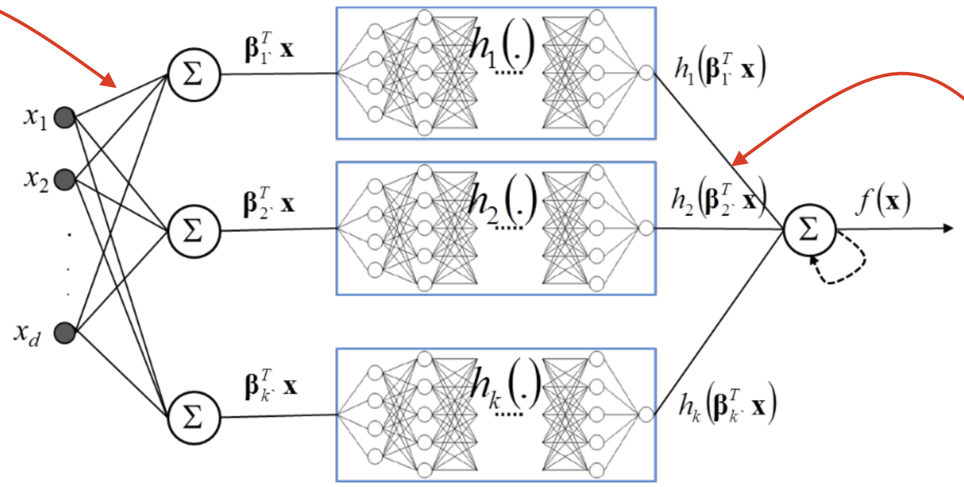
$B_j(.)$ with simple hinge functions are called ReLU (Rectifier Linear Units), $max(0,\, v_j\, x\text{-}c_j)$
c_j "knot locations" are called “bias weights”

Additive index structure for xNN

Additive 'Index' Model: $f(\mathbf{x}) = \gamma_1 h_1(\boldsymbol{\beta}_1^T \mathbf{x}) + \gamma_2 h_2(\boldsymbol{\beta}_2^T \mathbf{x}) + \ldots + \gamma_k h_k(\boldsymbol{\beta}_k^T \mathbf{x})$

Sparse

(and Orthogonal)



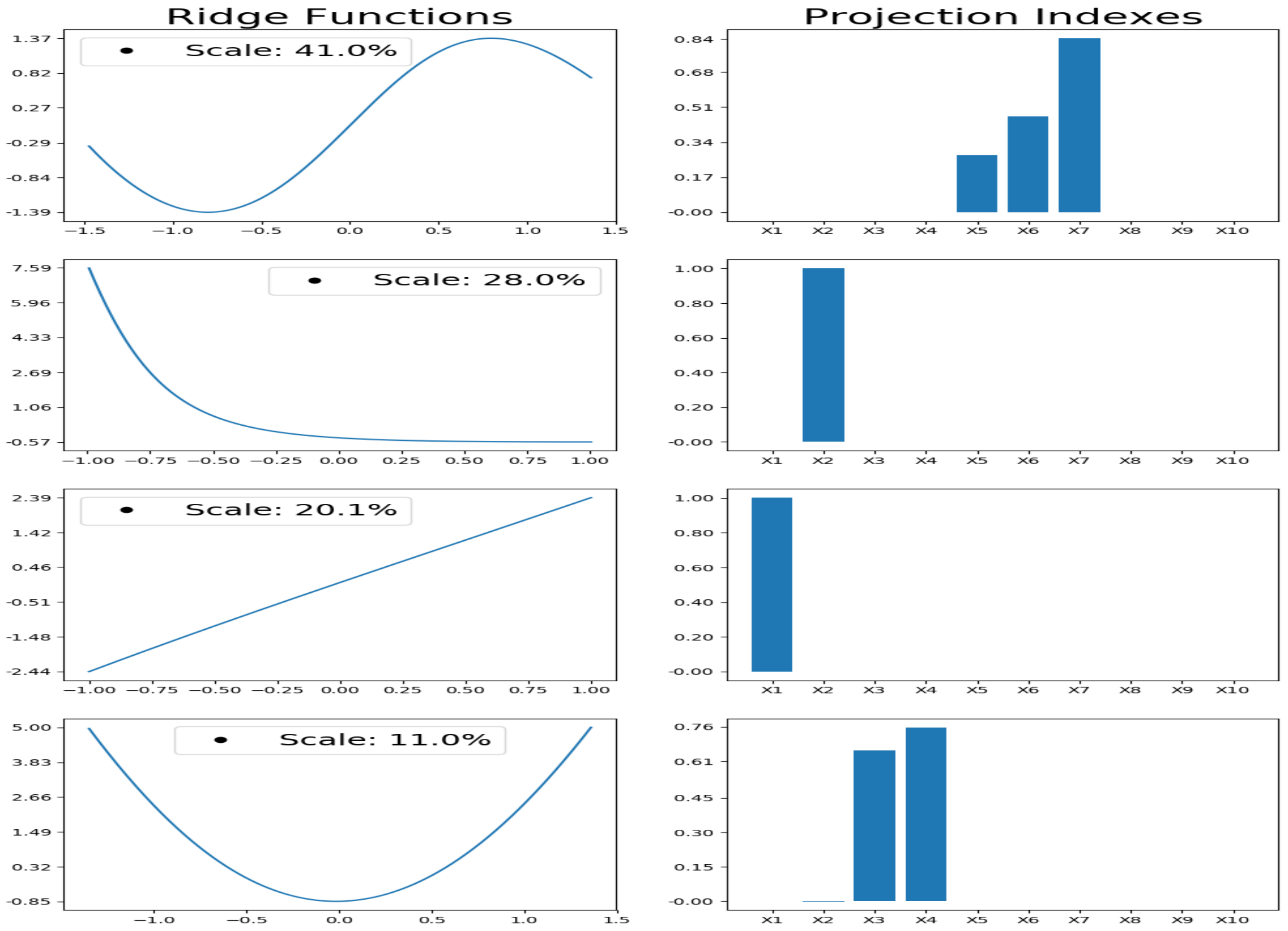
Sparse

Constraints can be introduced to Neural Networks architecture to improve interpretability:

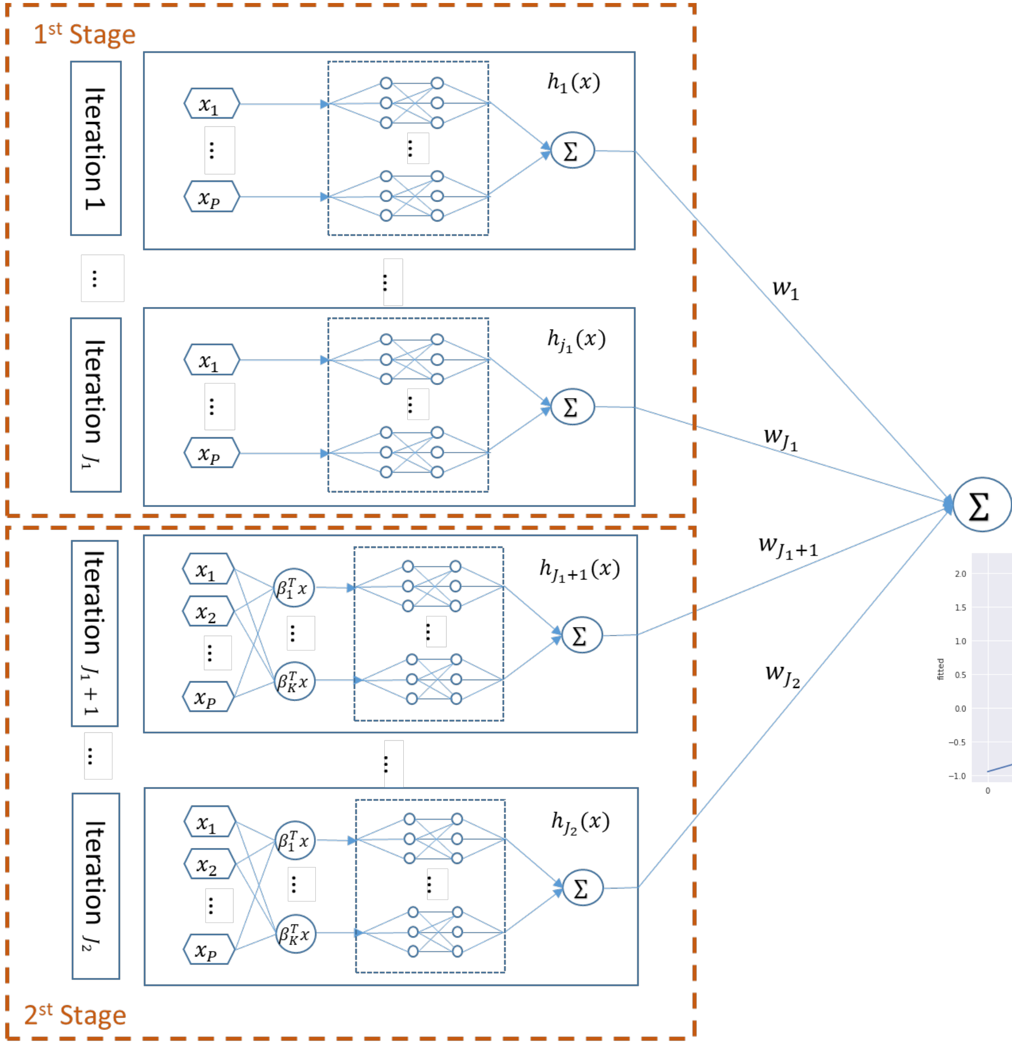
- Smaller number of nodes in the first layer
  - Projection Layer: Linear projections are interpretable
- Modularize the deeper layers (subnetworks)
  - Subnetwork: Nonlinear Ridge functions are easily graphed
- Additional constraints: sparsity and orthogonality

https://arxiv.org/pdf/1806.01933.pdf
https://arxiv.org/pdf/1901.03838.pdf

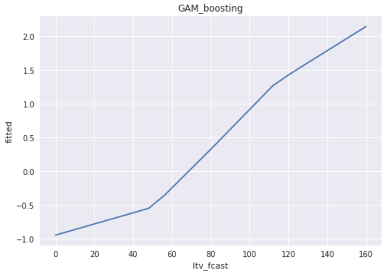
Example of xNN

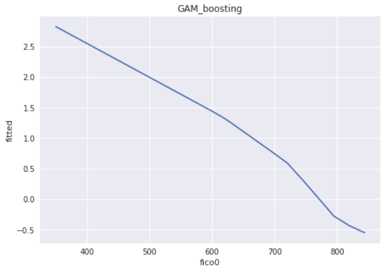


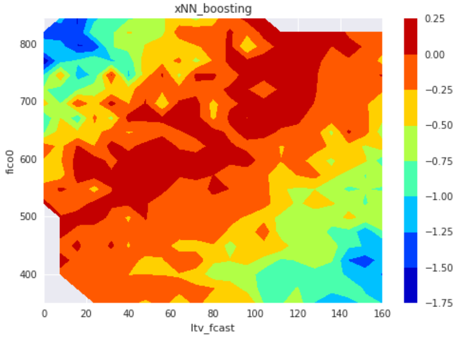
Adaptive explainable neural networks (AxNN)



- Stage 1 (Main Effects): Train GAM-Net with increasing ridge function complexity
- Stage 2 (Interaction Effects): Train xNN to capture interaction effects
- Iterations can be done by either 'boosting' or 'stacking' approach







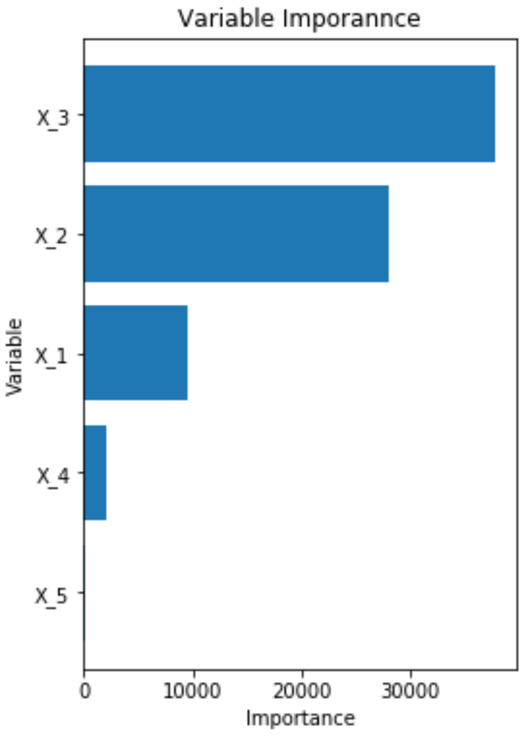
https://arxiv.org/ftp/arxiv/papers/2004/2004.02353.pdf
https://arxiv.org/pdf/2003.07132.pdf

Fully connected deep networks

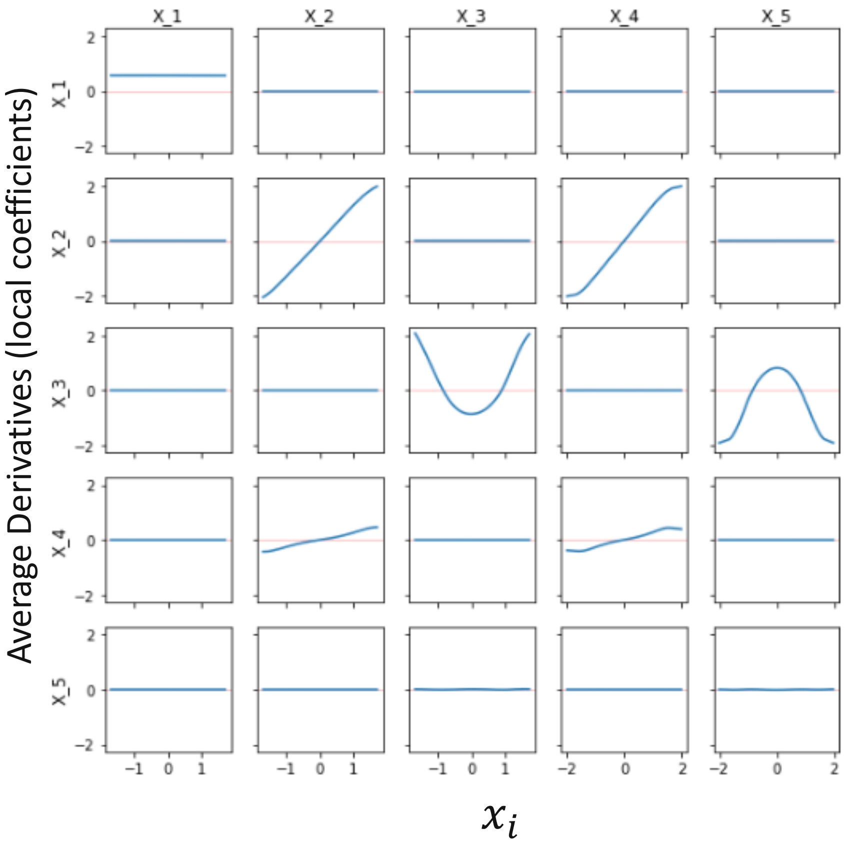
Deep networks with ReLU activation function can be decomposed into local linear models

- Local interpretation is exact: every point is associated with local linear model
- Global interpretation can be done by integrating (aggregating) local effects

Local interpretation



Global interpretation

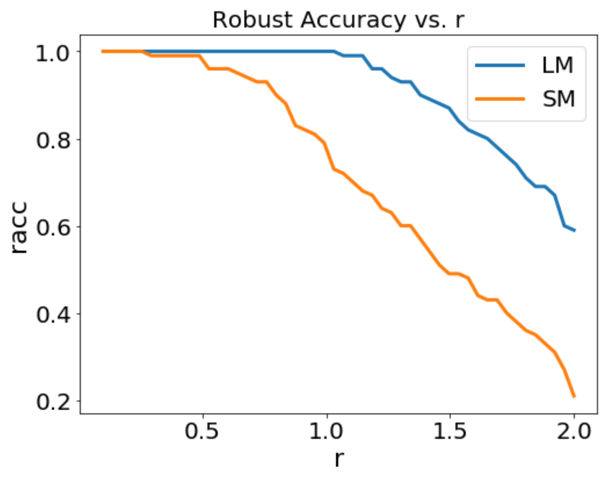


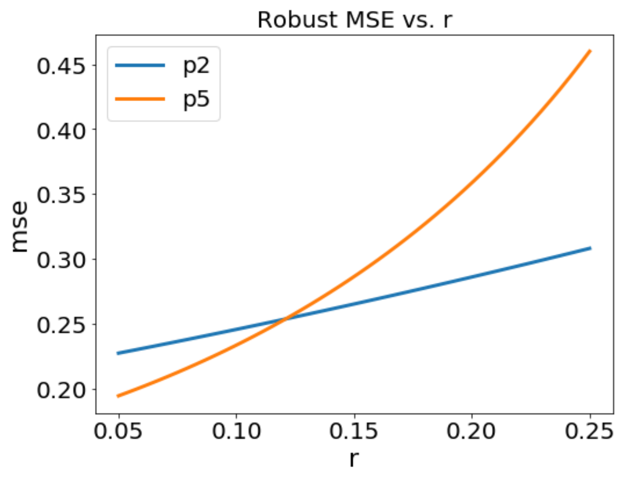
https://arxiv.org/ftp/arxiv/papers/1808/1808.07216.pdf

Model robustness test

- Building real world model is not Kaggle competition
- Current AutoML miss important aspect of reliable model
  - Solely focus on model performance and do not address model robustness
  - Data splitting (training-testing) is static: models in real worlds operate under dynamic (constantly changing) environment (e.g., population drift)
  - ML models such as NLP models can be susceptible to adversarial attack

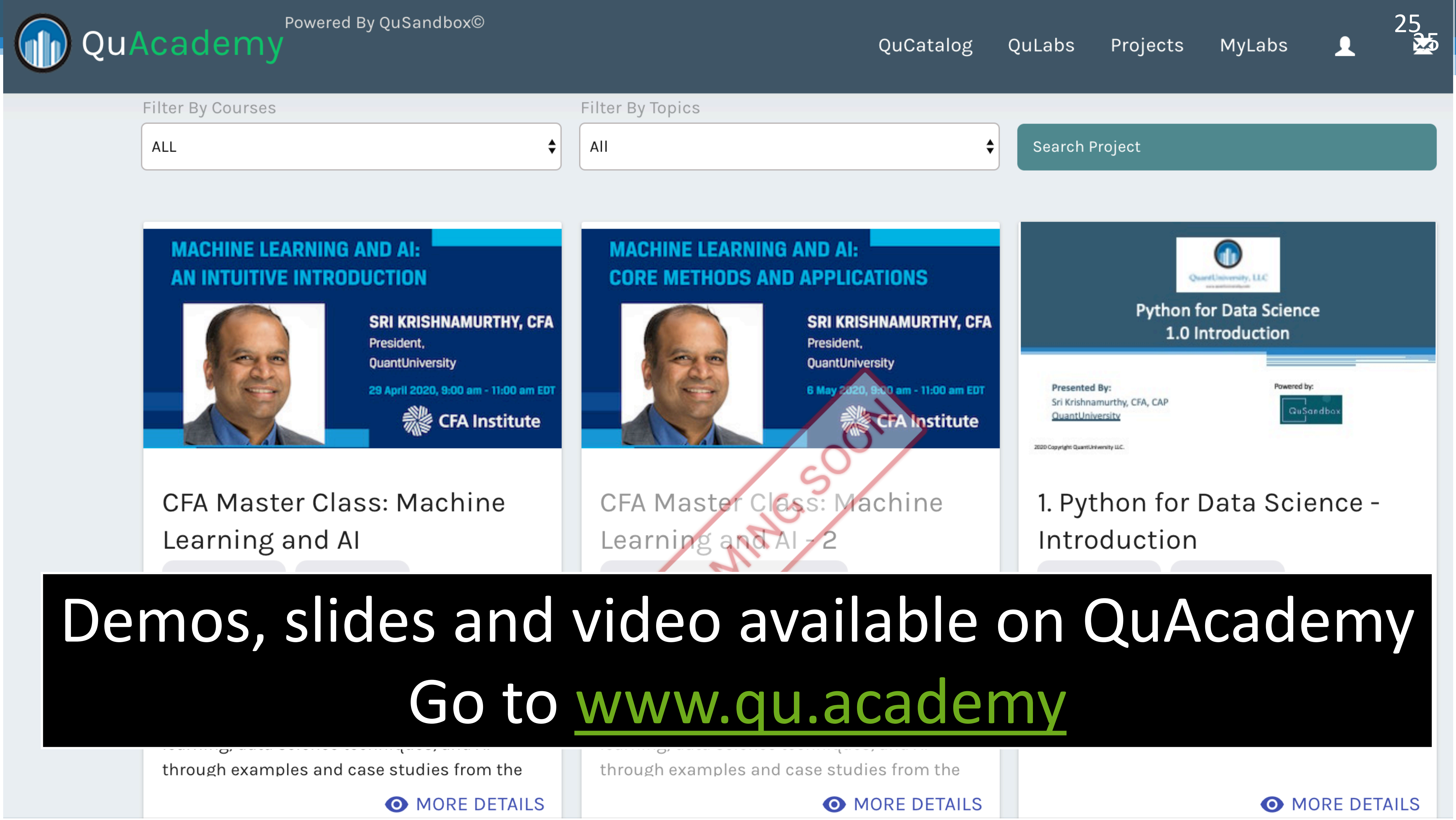
Define sensitive region $\mathcal{D}(r, \epsilon)$ as the region $\{x : \exists dx\ ||dx||_2 \leq r, \text{such that } \max_{dx} ||f(x+dx) - f(x)||_2 \geq \epsilon\}$





Governing Machine Learning Model Risk

- Policy and Procedure governing model life cycle
- Enterprise innovation team focus on AI strategy and coordination
- Model Development Center of Excellence
  - Centralized model development including vendor models
  - Dedicated development and deployment platform
- Model Validation standard and infra-structure
  - Dedicated Decision Science & Artificial Intelligence model validation team supported by Advanced Technology & Modeling team
  - Standardized model library and tests particularly for Fairness and Robustness
- Legal and Compliance review and approval



Demos, slides and video available on QuAcademy

Go to www.qu.academy

QU Speaker Series

Generating Synthetic Data with Generative Adversarial Networks (GANs)

Dr.Guilia Fanti Carnegie Mellon University

https://quspeakerseries4.splashthat.com/

QuantUniversity, LLC

www.quantuniversity.com

Wednesday, August 05 at 12:00pm

Dr.Guilia Fanti

Dr. Giulia Fanti is an Assistant Professor of Electrical and Computer Engineering at Carnegie Mellon University. Her research interests span the algorithmic foundations of blockchains, distributed systems, privacy-preserving technologies, and machine learning.

She is a fellow for the World Economic Forum's Global Future Council on Cybersecurity, and has received best paper awards from ACM Sigmetrics and ACM MobiHoc, as well as an NSF Graduate Research Fellowship.

Guilia is a recent recipient of the Faculty Research Award given by J.P.Morgan Chase on generating synthetic time series datasets

She obtained her Ph.D. in EECS from U.C. Berkeley and her B.S. in ECE from Olin College of Engineering.

QuantUniversity, LLC

www.quantuniversity.com

Thank you!

Contact

Sri Krishnamurthy, CFA, CAP
Founder and CEO
QuantUniversity LLC.

LinkedIn srikrishnamurthy

www.QuantUniversity.com

Information, data and drawings embodied in this presentation are strictly a property of QuantUniversity LLC. and shall not be distributed or used in any other publication without the prior written consent of QuantUniversity LLC.