From NP-Complete to NP-Hard:

Exploiting Mathematical Synergies between Electric Power Grid Operation and ML Verification

Sam Chevalier

University of Vermont

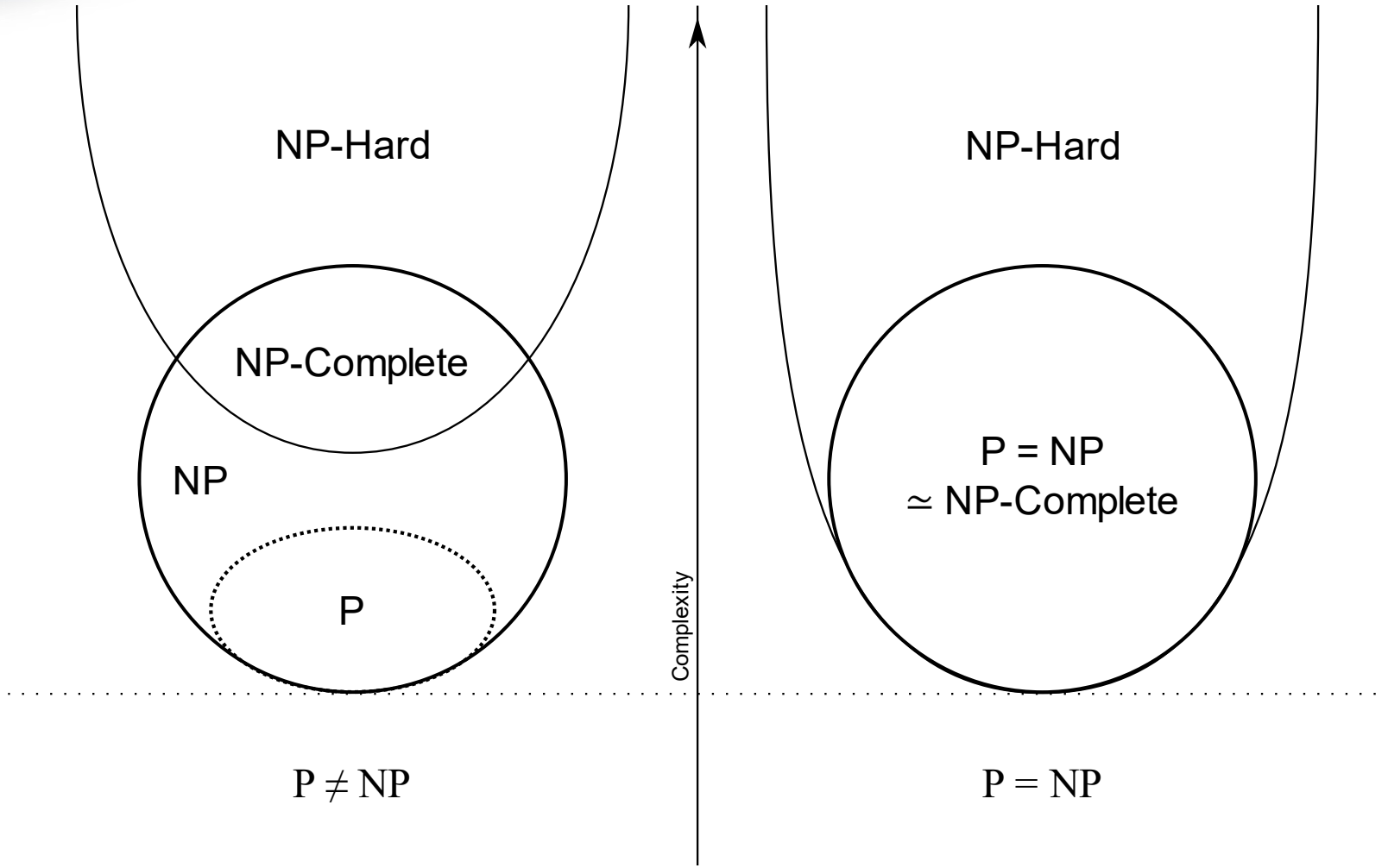
DTU Danmarks Tekniske Universitet

University of Vermont

Center for Energy and Autonomy CREATE College of Engineering and Mathematical Sciences

> Verifying DNNs is a difficult problem. DNNs are large, non-linear, and non-convex, and verifying even simple properties about them is an NP-complete problem (see Section I of the appendix). DNN verification is experimentally

Wikipedia:



[1] Katz, Guy, et al. "Reluplex: An efficient SMT solver for verifying deep neural networks." *CAV 2017.*

From NP-Complete to (NP-Hard $\wedge \notin$ NP)

Exploiting Mathematical Synergies between Electric Power Grid Operation and ML Verification

Sam Chevalier

University of Vermont

DTU Danmarks Tekniske Universitet

University of Vermont

Center for Energy and Autonomy CREATE College of Engineering and Mathematical Sciences

(Part of) What my lab at UVM focuses on

prove: (a) Operational guarantee

st: (b) neural network

(c) power grid physics

A Quick Historical Note on α,β-CROWN

Provably Bounding Neural Network Preimages

General Cutting Planes for Bound-Propagation-Based Neural Network Verification

Formal Verification for Neural Networks with General Nonlinearities via Branch-and-Bound

Beta-CROWN: Efficient Bound Propagation with Per-neuron Split Constraints for Neural Network

Automatic Perturbation Analysis for Scalable Certified Robustness and Beyond

A Branch and Bound Framework for Stronger Adversarial Attacks of ReLU Networks

⋮

αβ CROWN

Winner of International Verification of Neural Networks Competitions
(VNN-COMP 2021, 2022, 2023)

Efficient Neural Network Robustness Certification with General Activation Functions

Huan Zhang[1,3,†,*] Tsui-Wei Weng[2,†] Pin-Yu Chen[3] Cho-Jui Hsieh[1] Luca Daniel[2]

My PhD Advisor!

Lecture (Talk?) Outline

①

Challenges

...in actual, and future, power systems.

②

Tools

...for overcoming these challenges (ML + verification)

③

Synergies

...between ML verification and grid operation.

Lecture (Talk?) Outline

①

Challenges

...in actual, and future, power systems.

②

Tools

...for overcoming these challenges (ML + verification)

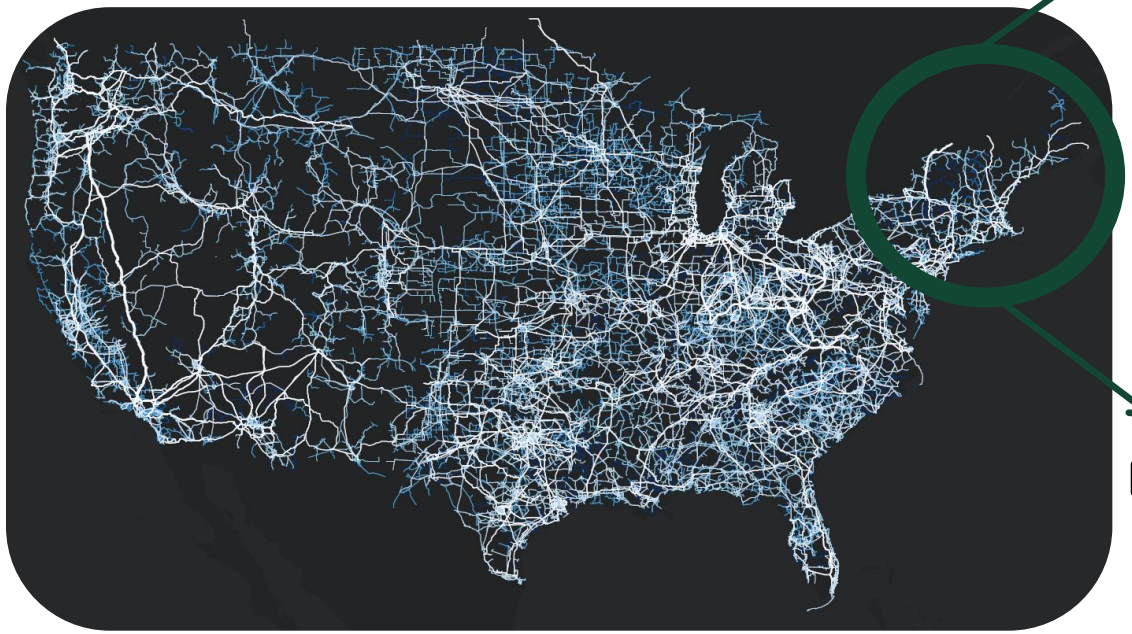
③

Synergies

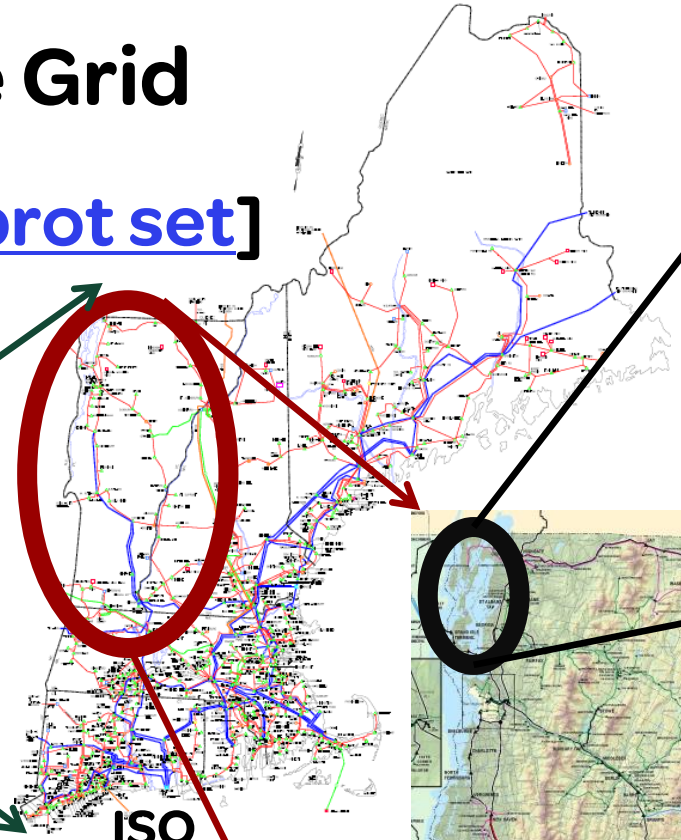
...between ML verification and grid operation.

Challenges in Operating the Grid

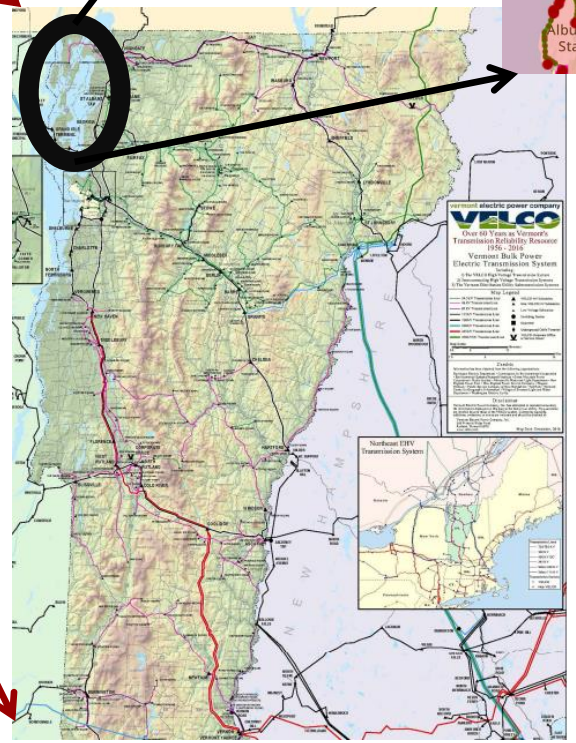
The “grid” is **[a]** huge **[Mandelbrot set]**



Western Interconnect, Eastern Interconnect, and Texas



ISO New England



VELCO (Vermont)

VEC (South Alburgh) Almost 10k nodes!

Challenges in Operating the Grid

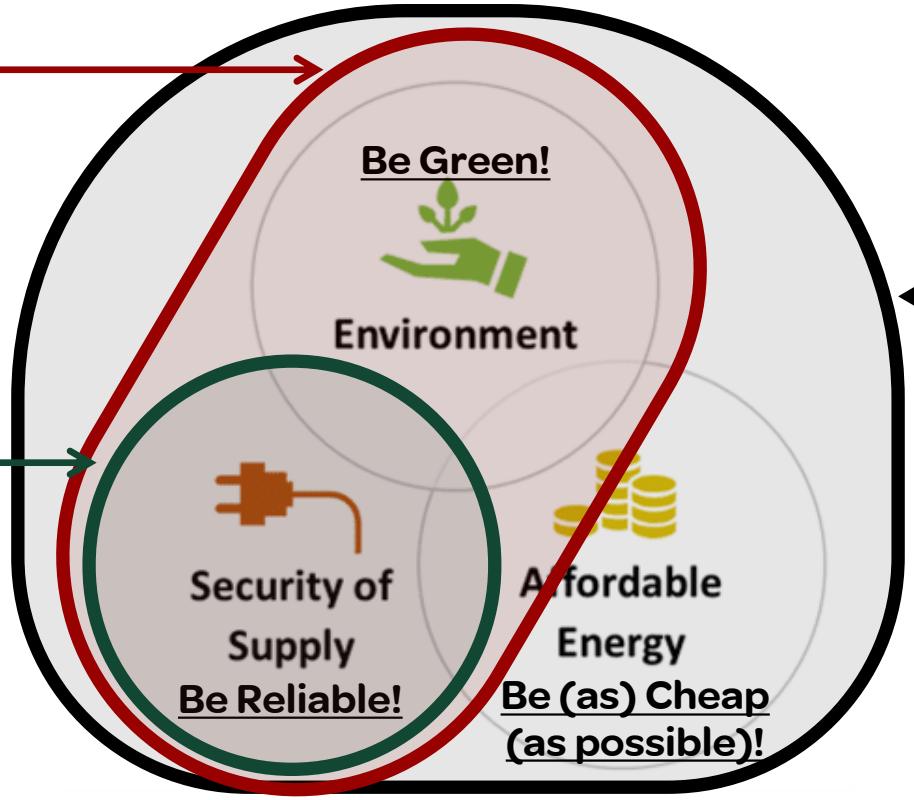
Grids operation has three **competing** goals: cheap, reliable, green.

- Which one do you think **dominates**?

More Constraints! Solution can be verified quickly, but still NP-Hard(er)

A given solution can be verified in Polynomial time, but still NP-Hard [1]

[one-in-three 3-SAT problem]



NP-Hard and NOT verifiable in polynomial time

$\ldots \wedge \notin \mathbf{NP}$

[1] Bienstock, Daniel, and Abhinav Verma. "Strong NP-hardness of AC power flows feasibility." *Operations Research Letters* 47.6 (2019).

Quick Evidence of NP-Hardness…

GRID OPTIMIZATION COMPETITION

ARPA-E GO Competition: the hardest, meanest, ugliest gird optimization challenge in the world.

Given 6+ hours on a super-computer, no team could find **feasible** solutions on the largest, 23k-bus power system in multiple scenarios

- Feasible solutions do, theoretically, exist

model	scenario	SW	Best Team	Best Score	ARPA-e Benchmark	Artelys_Columbia	GOT-BSI-OPF	quasiGrad	TIM-GO	YongOptimization
C3E4N23643D1	**3**	1	TIM-GO	104,686,125	61,152,061	63,340,112	99,123,868	48,878,908	104,686,125	104,073,565
C3E4N23643D1	4	1	GOT-BSI-OPF	91,584,129	0	70,444,810	91,584,129	0	39,494,965	69,793,156
C3E4N23643D2	**3**	1	YongOptimization	600,577,211	0	353,804,820	589,696,576	598,132,224	588,991,290	600,577,211
C3E4N23643D2	4	1	**none**	0	0	0	0	0	0	0
C3E4N23643D3	**3**	1	YongOptimization	2,158,212,496	0	1,162,674,657	2,093,288,847	2,143,434,855	2,112,949,852	2,158,212,496
C3E4N23643D3	4	1	**none**	0	0	0	0	0	0	0
C3E4N23643	**6**	#	**(all) ensemble**	**2,955,059,960**	**61,152,061**	**1,650,264,399**	**2,873,693,419**	**2,790,445,988**	**2,846,122,232**	**2,932,656,427**
C3E4N23643D1	**2**	#	**D1 ensemble**	**196,270,254**	61,152,061	133,784,922	190,707,997	48,878,908	144,181,090	173,866,721
C3E4N23643D2	**2**	#	**D2 ensemble**	**600,577,211**	0	353,804,820	589,696,576	598,132,224	588,991,290	600,577,211
C3E4N23643D3	**2**	#	**D3 ensemble**	**2,158,212,496**	0	1,162,674,657	2,093,288,847	2,143,434,855	2,112,949,852	2,158,212,496

...and the savings could be huge!

GRID OPTIMIZATION COMPETITION

- In the early 2000s, power system operators began switching from **Lagrangian Relaxation** to **Mixed Integer Program** solvers

  – e.g., Gurobi, CPLEX, etc.

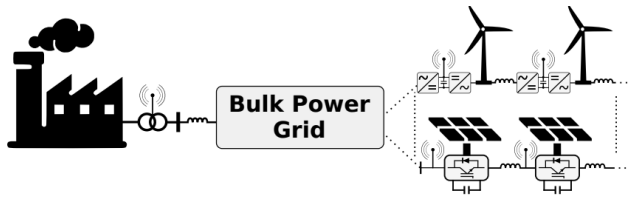
- By 2011, this was saving US grid operators **$500 million** per year [1]

- Robert Bixby (CLPEX and Gurobi founder) met Dick O'Neil at the 1999 Discrete Mathematics and Theoretical Computer Science meeting, and MIP-based **Unit Commitment** was born

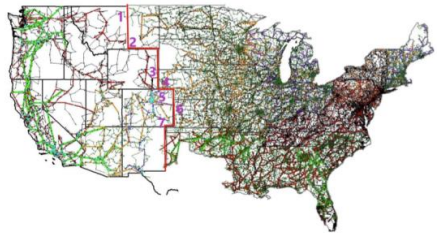
[1] Cain, M. B., R. P. O'Neill, and A. Castillo. "Optimal power flow papers: Paper 1. History of optimal power flow and formulations." *Federal Energy Regulatory Commission, Tech. Rep* (2013).

Challenges in Operating the Grid

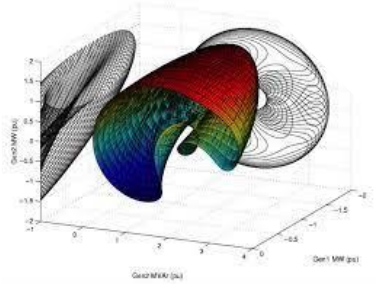
The grid has well-modeled, but complicated, physics



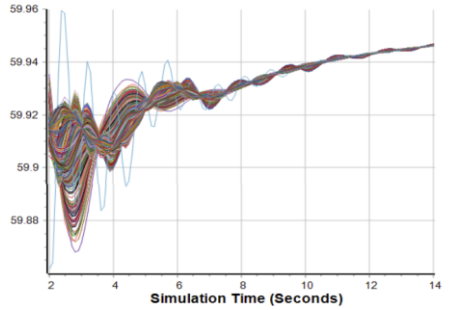
Renewable dynamics



Network flows



Voltage stability



Transient response

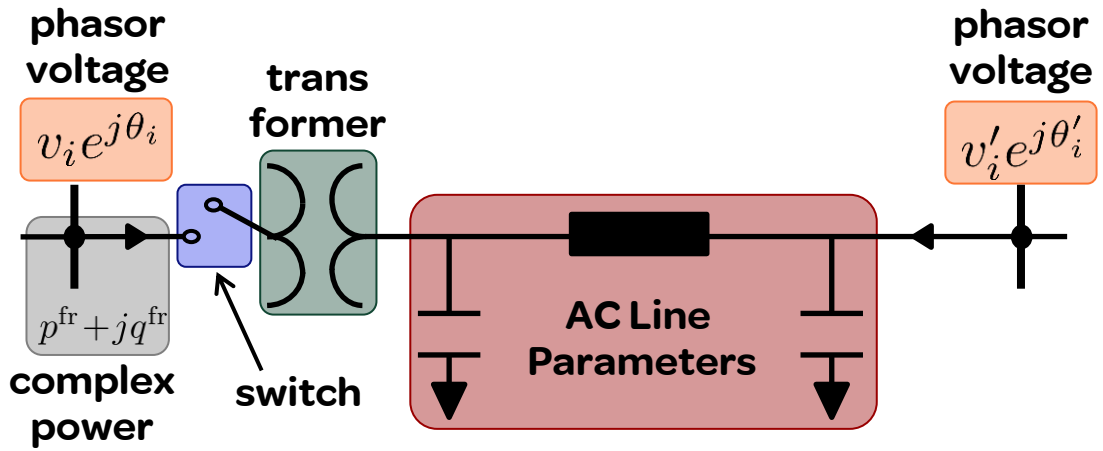
In this talk, we will focus on "quasi-steady state" **power flow** physics:

$$
\begin{aligned}
p^{\mathrm{fr}}_{jt} &= u^{\mathrm{on}}_{jt}\left(\left(g^{\mathrm{sr}}_j + g^{\mathrm{fr}}_j\right) v^2_{it}/\tau^2_{jt} + \left(-g^{\mathrm{sr}}_j \cos\left(\theta_{it} - \theta_{i't} - \phi_{jt}\right)\right.\right. \\
&\quad \left.\left. - b^{\mathrm{sr}}_j \sin\left(\theta_{it} - \theta_{i't} - \phi_{jt}\right)\right) v_{it} v_{i't}/\tau_{jt}\right) \\
q^{\mathrm{fr}}_{jt} &= u^{\mathrm{on}}_{jt}\left(\left(-b^{\mathrm{sr}}_j - b^{\mathrm{fr}}_j - b^{\mathrm{ch}}_j/2\right) v^2_{it}/\tau^2_{jt} + \left(b^{\mathrm{sr}}_j \cos\left(\theta_{it} - \theta_{i't} - \phi_{jt}\right)\right.\right. \\
&\quad \left.\left. - g^{\mathrm{sr}}_j \sin\left(\theta_{it} - \theta_{i't} - \phi_{jt}\right)\right) v_{it} v_{i't}/\tau_{jt}\right)
\end{aligned}
$$

ACOPF Polar form: $\sim v_i v_j \cos(\theta)$

Rectangular form: $\sim V_r V_i$

} **Pick your poison!**



Challenges in Operating the Grid

Thankfully, simplifications are used! Out of computational *necessity:*

$$p_{ii'} = v_i v_{i'} (g_{ii'} \cos(\theta_i - \theta_{i'}) + b_{ii'} \sin(\theta_i - \theta_{i'}))$$

$$\approx b_{ii'} (\theta_i - \theta_{i'})$$ **: Line flow is proportional to angle differences**

- This is the linear "DC" power flow approximation, and it is basis of network optimization. Example: the DC "optimal power flow" (OPF) dispatches generators to meet demand, while respecting flow limits:

$$\min p_g^T c_g$$

$$\text{s.t.} \sum p_g = \sum p_d : \lambda$$

$$\underline{p}_g \leq p_g \leq \overline{p_g}$$

$$\underline{p}_f \leq B p_{g-d} \leq \overline{p}_f : \mu$$

Power Transfer Distribution Factor (PTDF) matrix

Using the duals at optimality, Locational Marginal Prices (LMPs = cost of power at any point in the grid) "pop" out!

$$\text{LMP} = \lambda + B^T \mu$$

"There is a need for fundamental changes in the ways society views electric energy. Electric energy must be treated as a **commodity** which can be bought, sold, and traded, taking into account its time- and space-varying values and costs... The framework is based on the use of spot prices." **Schweppe**, Fred C., et al. *Spot pricing of electricity*. 1988.

Challenges in Operating the Grid

This is not just academic fluff: this is how grids are actually run (e.g., Texas):

The SCED Optimization Objective Function and Constraints

The SCED optimization objective function is as given by the following:

Minimize { Cost of dispatching generation
+ Penalty for violating Power Balance constraint
+ Penalty for violating transmission constraints}

which is:

Minimize {sum of (offer price * MW dispatched)
+ sum (Penalty * Power Balance violation MW amount)
+ sum (Penalty *Transmission constraint violation MW amount) }

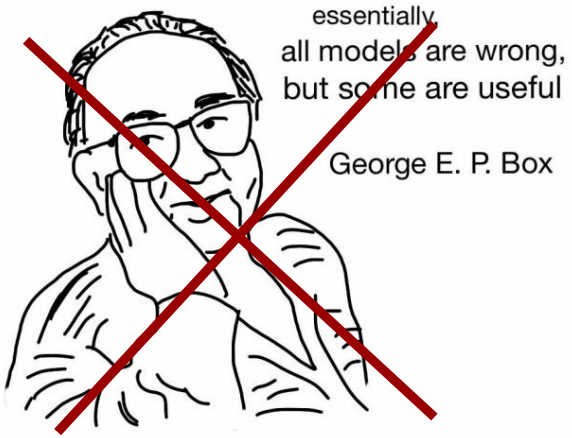
The objective is subject to the following constraints:

- Power Balance Constraint
  sum (Base Point) + under gen slack – over gen slack = Generation To Be Dispatched
- Transmission Constraints
  sum(Shift Factor * Base Point) – violation slack ≤ limit
- Dispatch Limits
  LDL ≤ Base Point ≤ HDL

ERCOT Public

Based on the SCED dispatch the LMP at each Electrical Bus is calculated as

$$LMP_{bus,t} = SP_{demand,t} - \sum_{c} SF_{bus,c,t} \cdot SP_{c;t}$$



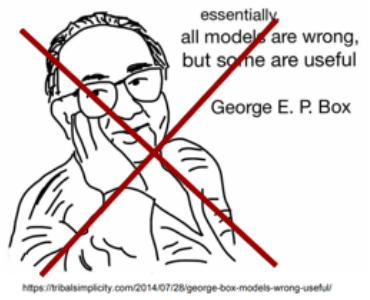
https://tribalsimplicity.com/2014/07/28/george-box-models-wrong-useful/

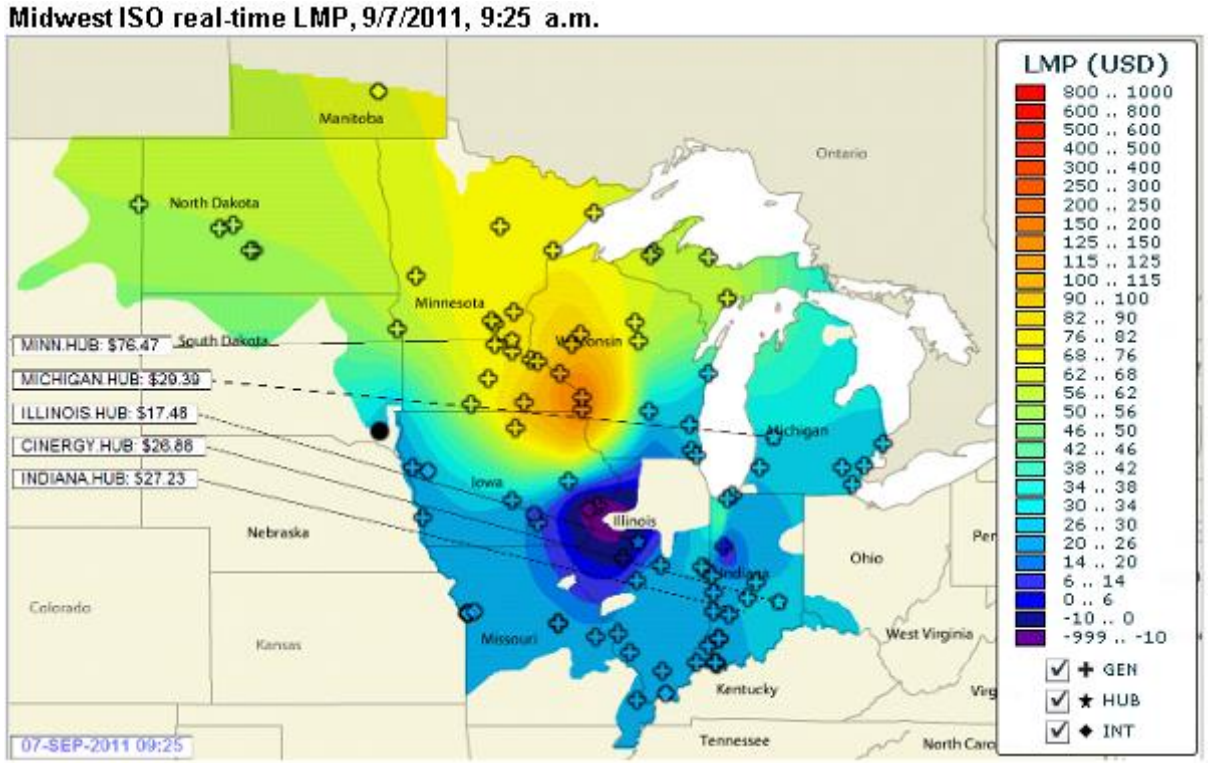
Challenge I: Keep Prices Low

The dual variables of the DCOPF problem provide network prices, paid for by wholesale market participants (generators, utilities; not you)

- Remember: global price minimization is not in NP!

- ERCOT prices
- PJM Prices
- MISO (you!) prices





Challenge I: Keep Prices Low

NONCONVEX MARKETS DRIVE POWER SYSTEMS

MISO

Solution Accuracy Requirement:

"DA MIP relative gap ≤ 0.1%"

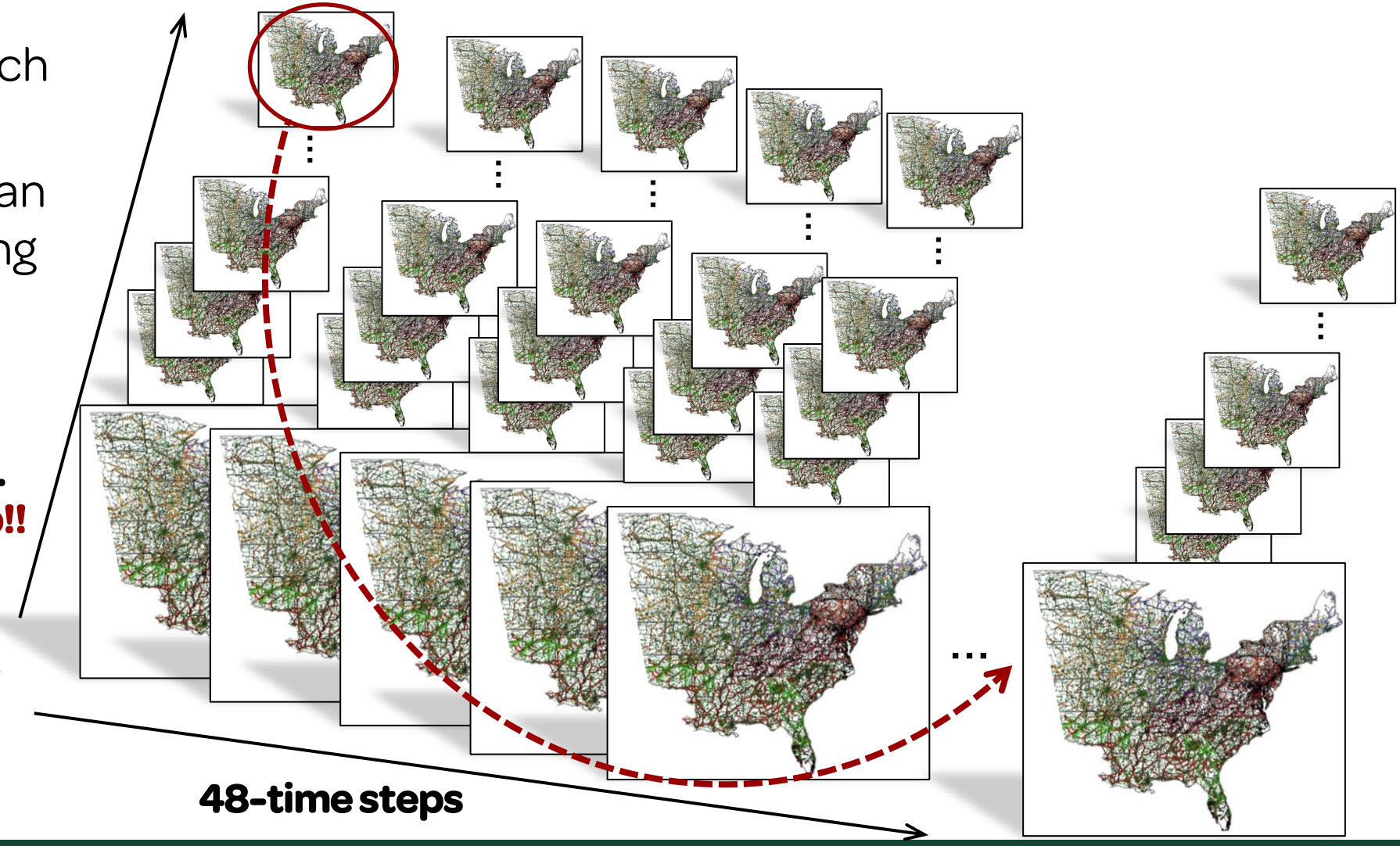
"What-if" analysis on commitment justifications

- Avoid participants' dispute on "out-of-the-money" resources.
- May lead to adjustment on disputable commitment results due to MIP gap
  - e.g. not committing wind units with close to 0 cost since the impact to the objective is less than MIP gap

Challenge II: "Security Constraints" for Network Reliability

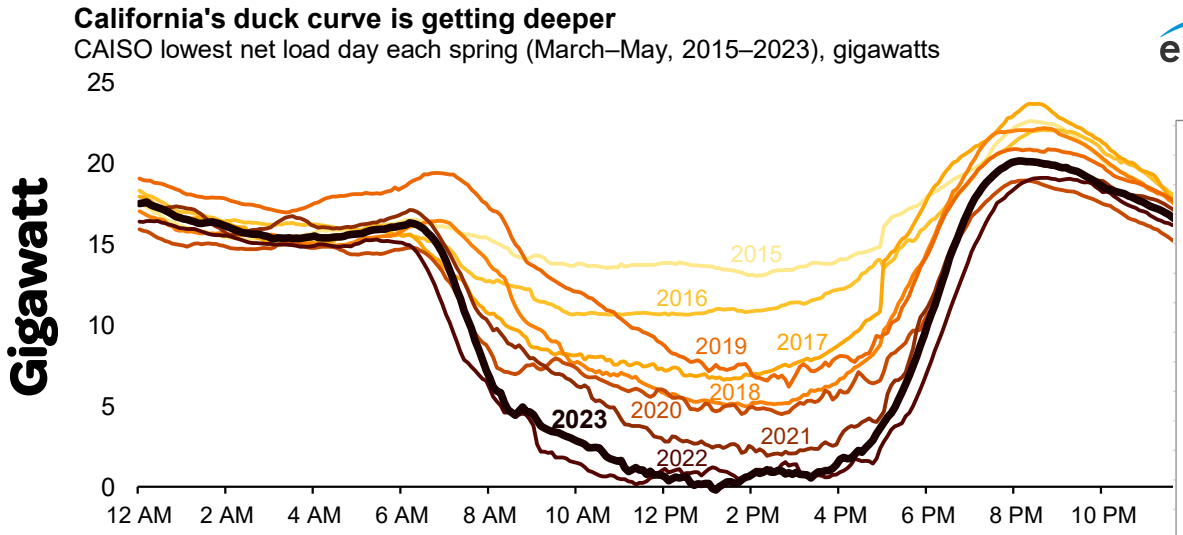
- Challenge: find an operating condition which is "N-1" secure
- Meaning: any **one line** can be lost without sacrificing network integrity
- Largest GO testcase:
  23,000+ contingencies…
  at each time step!!
- Hard problem, but its solution is easy to verify

  "$\in$ NP"



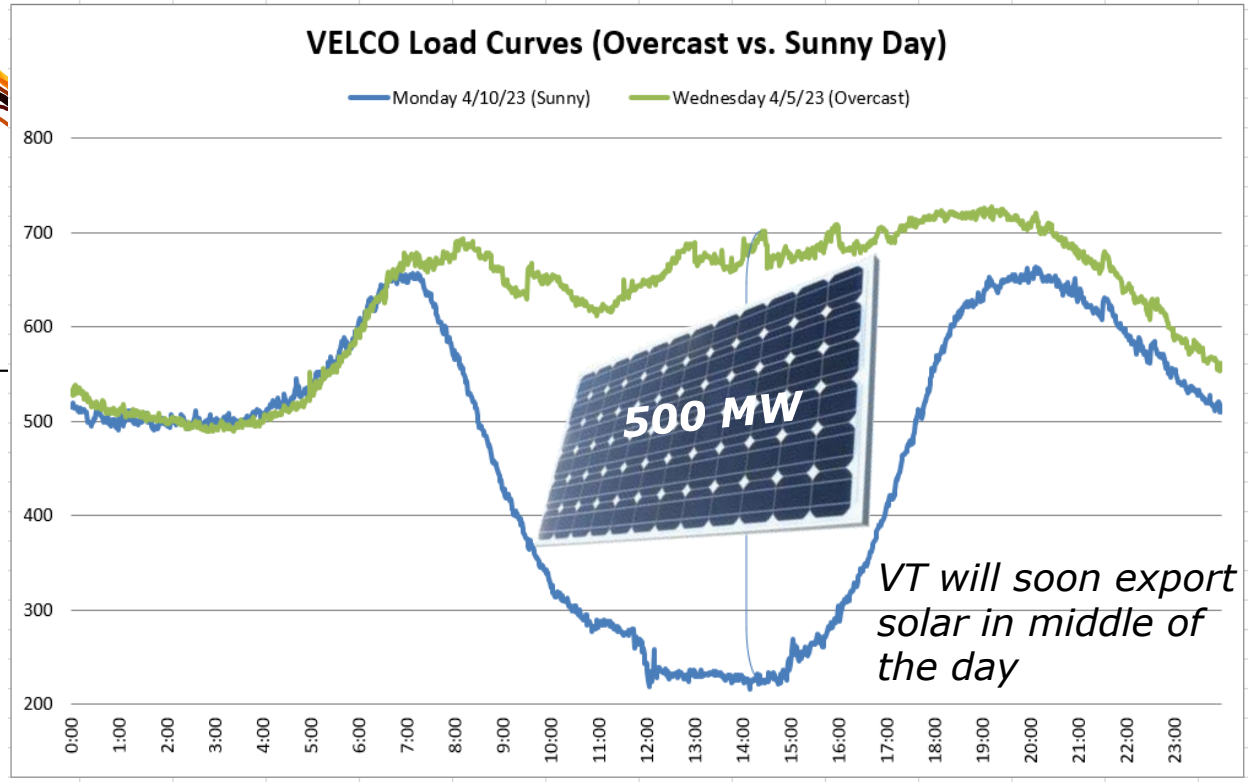
Challenge III: Renewables are coming…

California's "duck" curve is coming for you:



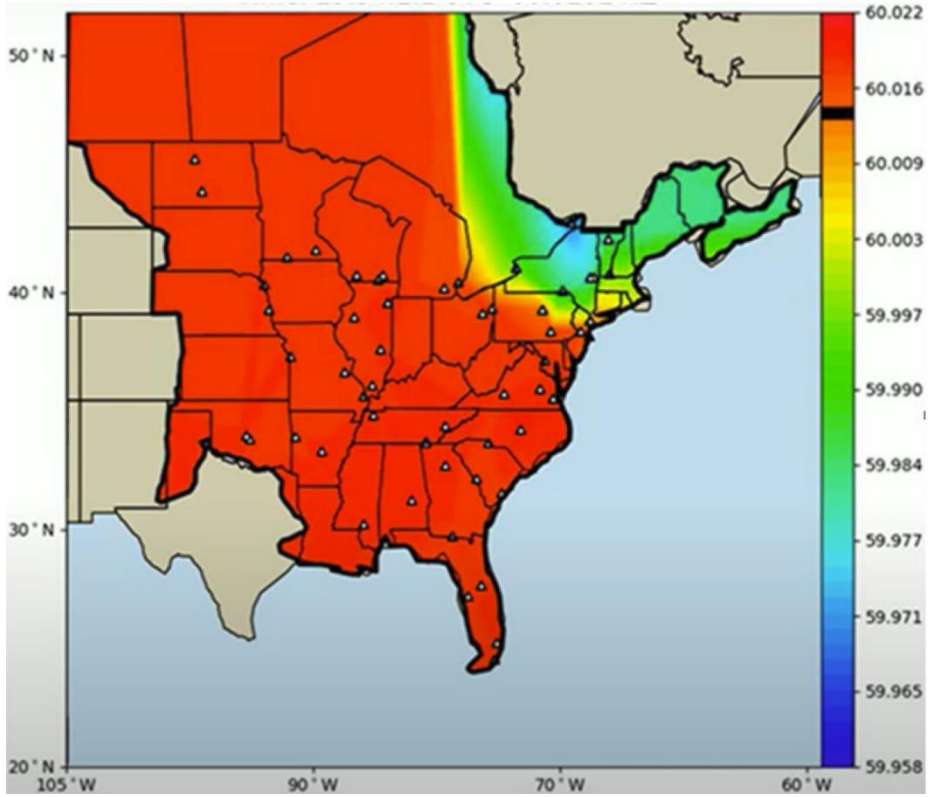
eia

And so is Vermont's Champ curve!!



Challenge III: Renewables are coming…

Potential consequences: the transmission grid is at the mercy of **distributed energy resource (DER)** behavior



- Summer of 2022: HVDC line connecting NY and Canada tripped offline, leading to DER trip
- Vermont net load **increased by 10%,** because it lost so much small-scale solar
- DERs will soon dominate the grid

Open Challenges in Operating the Grid [Sam's top 4]

1. Convex relaxation-based global optimization solutions (i.e., Semidefinite Programming) are generally not "tight"/feasible
   - Also, Mixed Integer SDP solvers don't really exist

     MOSEK can perform mixed-integer linear (MILO) and conic (MICO) problems, except for mixed-integer semidefinite problems.

2. AC transmission line switching is extremely hard.
   - Relaxations are useless. Most GO teams didn't even bother.

3. If a problem is true bilevel optimization problem, forget it
   - In a day of bitcoin and data centers, how do we solve this? Loads are flexible functions of LMP! Nasty.

4. Faster bound tightening [more later]

$$\min c_g^T p_g$$
$$\text{s.t.} \sum p_g = \sum p_d$$
$$\underline{p} \leq B p_{g-d} \leq \overline{p}$$
$$p_{d,i} = f(\text{LMP}_i)$$

Lecture (Talk?) Outline

①

Challenges

...in actual, and future, power systems.

②

Tools

...for overcoming these challenges (ML + verification)

③

Synergies

...between ML verification and grid operation.

[Quick aside 1: Verification is like Optimization]

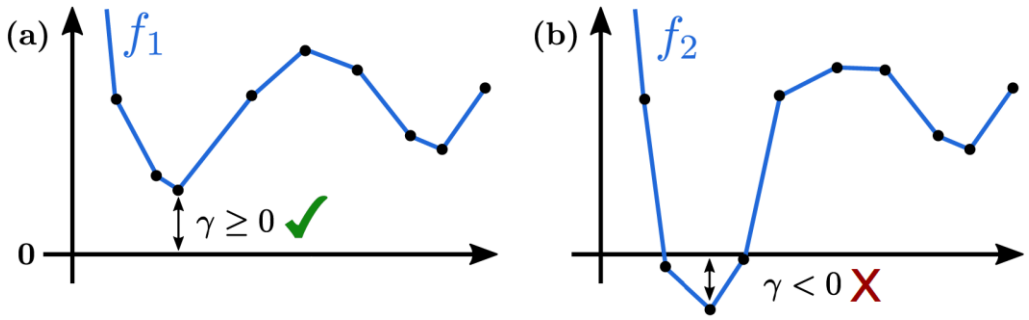
- Every verification problem can be posed in this form:

$$\gamma = \min_{x \in \mathcal{C}} f(x)$$

- If the metric is everywhere satisfied, the NN is "verified":

$\gamma \geq 0 \Rightarrow$ metric verified **(pass)** ✓

$\gamma < 0 \Rightarrow$ counter example found **(fail)** X



✓The **sign** of γ represents a verification result (yes/no)

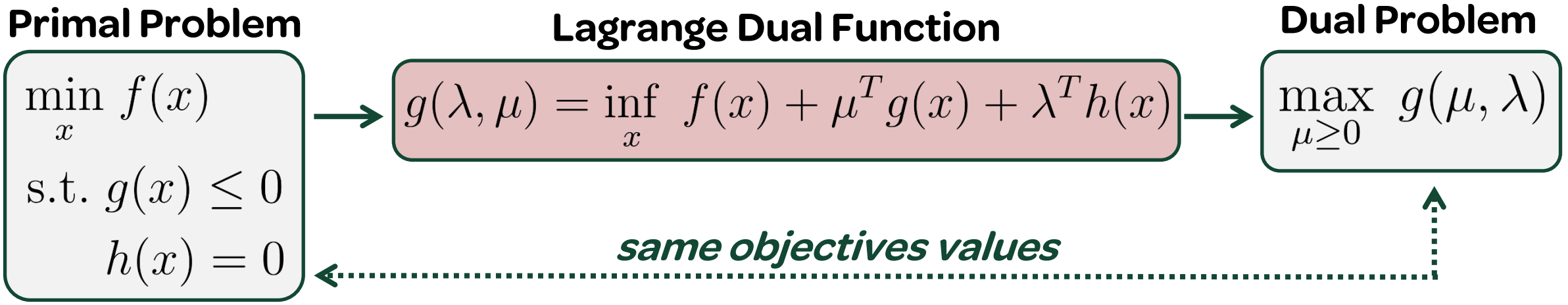
✓The **value** of γ represents a "worst case performance guarantee"

- **Challenge:** NNs are "spikey" and can yield highly nonconvex objectives

[Quick aside 2: Verification Exploits Dual Formulations]

Given a convex* problem, the **primal** and **dual** objectives are equal in value

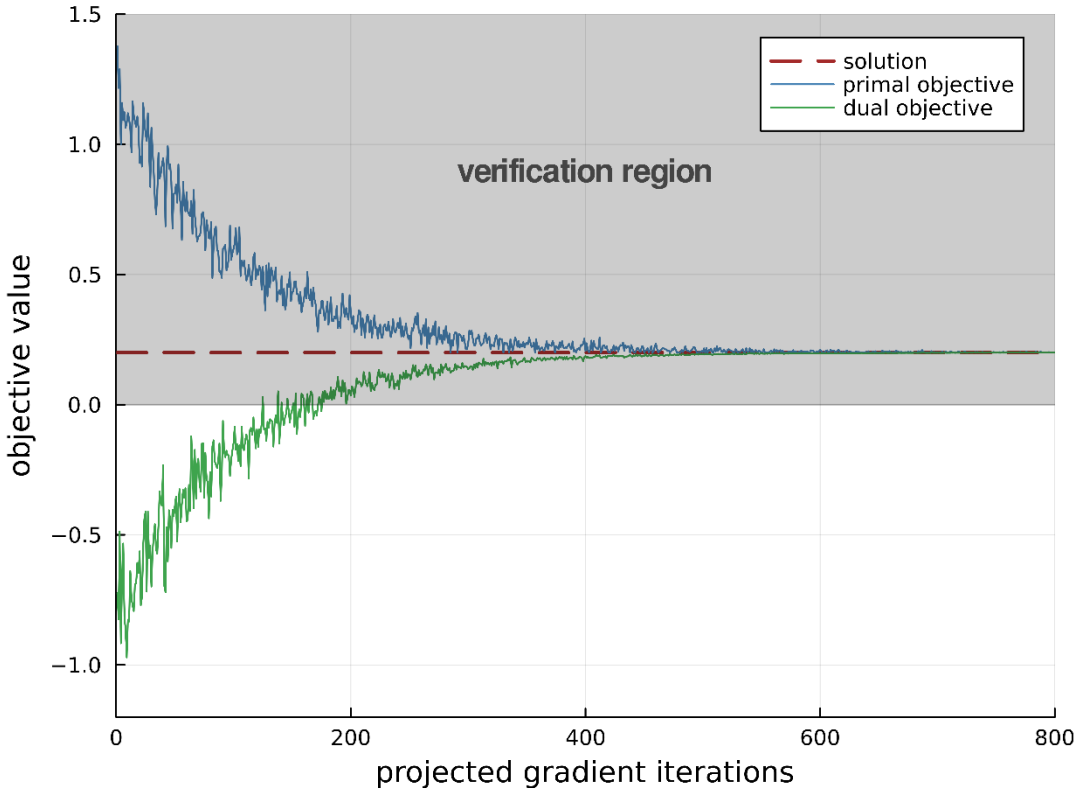
- From Boyd & Vandenberghe:



- In the NN verification problem, we care about **objective bounds**, so the primal and the dual problems can both be useful

[Quick aside 3: Verification Exploits Dual Formulations]

Assume you can solve the **primal** or **dual** with a projected gradient method:



Primal: $\min\ f(x),\ \text{s.t...}$

✓ obvious to formulate

✓ feasible iterates give a "worst incumbent"

X "bound" only guaranteed at convergence

Dual: $\max\ g(\mu, \lambda),\ \text{s.t...}$

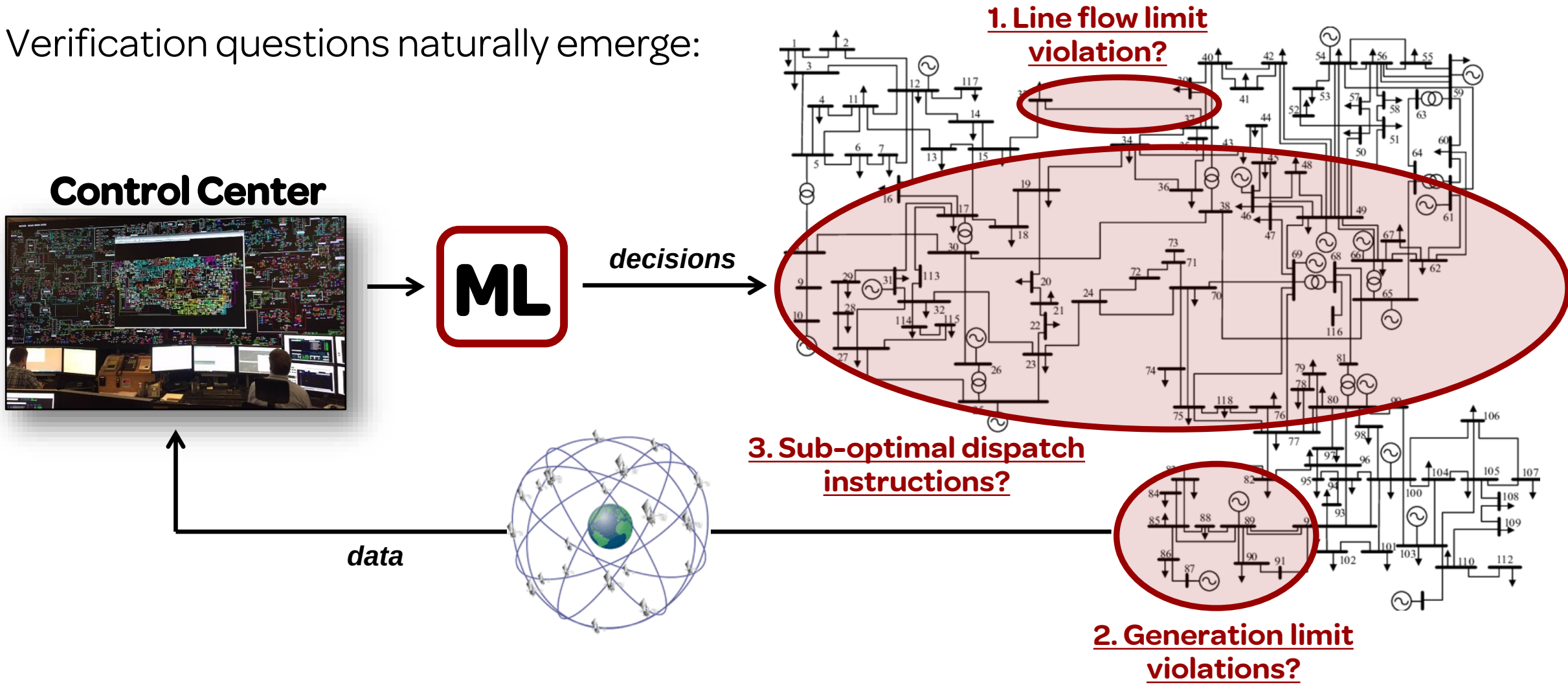
X "what the heck is the dual...?" - AP

✓ feasible iterates lower bound performance

✓ terminate early if crosses 0 (pre-converge)!

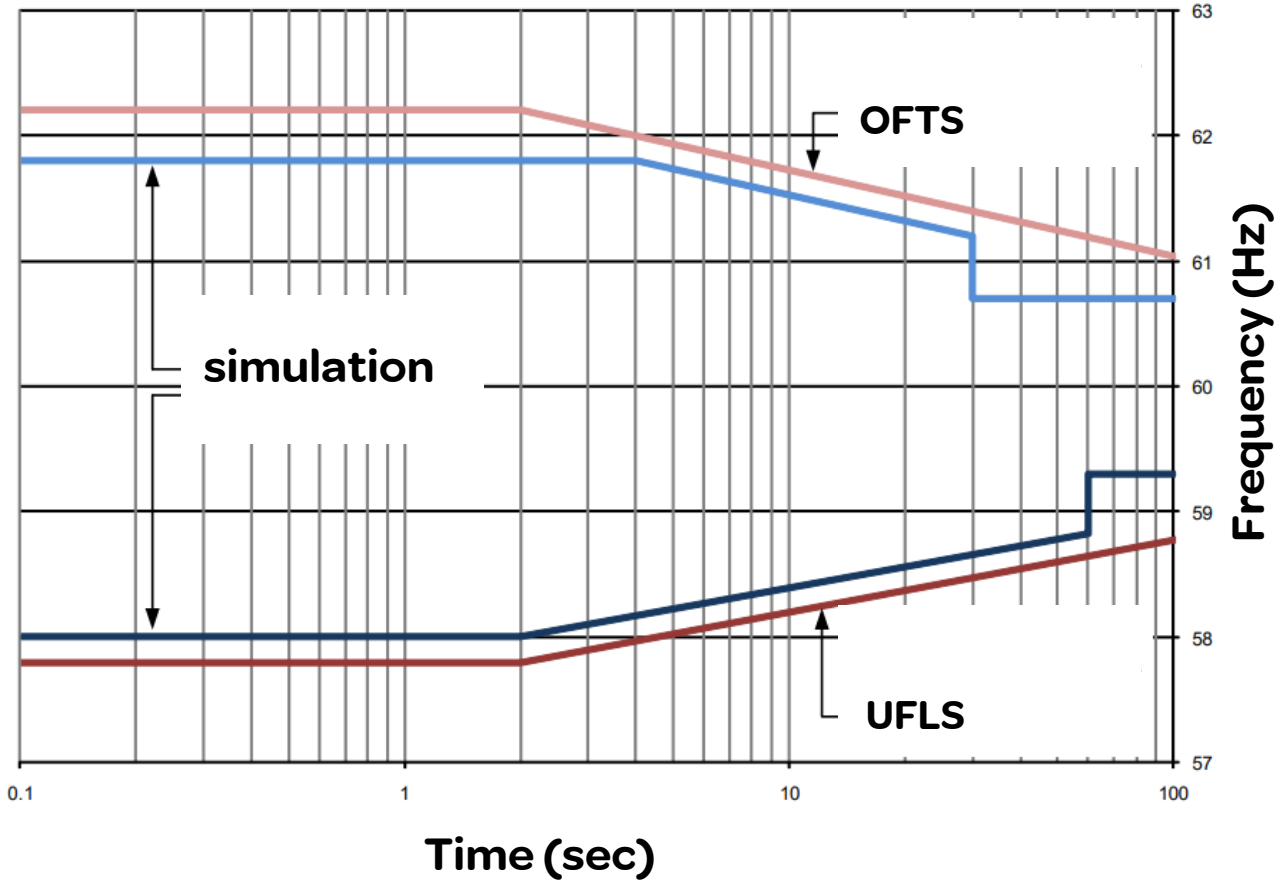
Tools: ML to the Rescue…?

- Future grids envision **ML** models "in the operational loop"
- Verification questions naturally emerge:



Tools: ML to the Rescue...? Compliance is king!!!

PRC6: Automatic Underfrequency Load Shedding

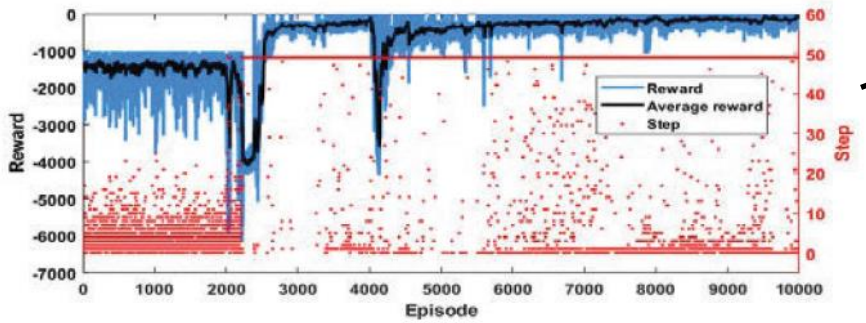


- Vermont Transmission Operators want adaptive UFLS parameter tuning to limit DER shedding
- Adaptive UFLS may be better than traditional tuning, but it must be **guaranteed to meet compliance targets**, enforced by NERC
- **Verification** of data-driven schemes can be used to ensure compliance

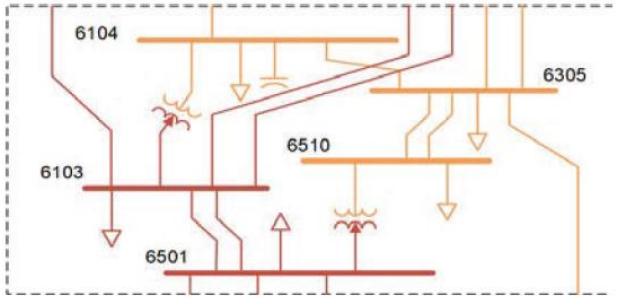
Tools: ML to the Rescue...?

Reinforcement Learning Based Voltage Control Using Multiple Control Devices

Yuling Wang[1], Vijay Vittal[1], Xiaochuan Luo[2], Slava Maslennikov[2], Qiang Zhang[2], Mingguo Hong[2], Song Zhang[3]
[1]School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ, USA
[2]Advanced Technology Solutions, ISO New England, Holyoke, MA, USA
[3]Energy & Utilities, Amazon Web Services, Seattle, WA, USA



Train an RL agent to make complex voltage control decisions



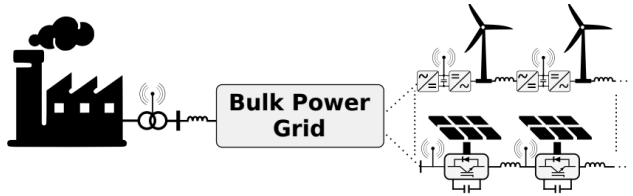
But, how can they trust it...? How about we solve this:

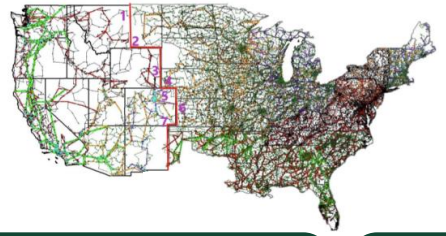
$$
\begin{aligned}
\max \quad & \textbf{network voltage violation} \\
\text{s.t.} \quad & G, B = \mathrm{NN}(v, p, q) \\
& p_i = v_i \sum v_k (G_{ik} \cos(\theta_{ik}) + B_{ik} \sin(\theta_{ik})) \\
& q_i = v_i \sum v_k (G_{ik} \sin(\theta_{ik}) - B_{ik} \cos(\theta_{ik}))
\end{aligned}
$$

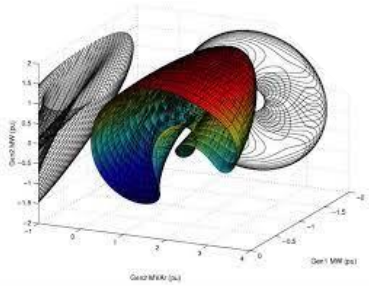
→ Negative system impacts
→ RL decisions
→ Network physics

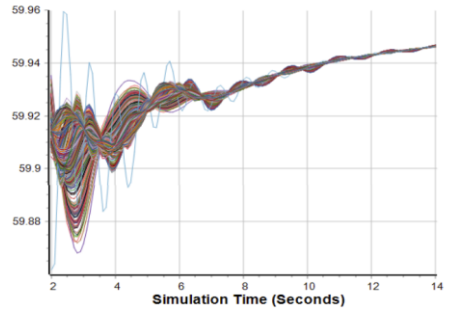
Verification in Power Systems — Opportunities

Key observation: In power systems, we know the physics!









Worst-Case Performance:

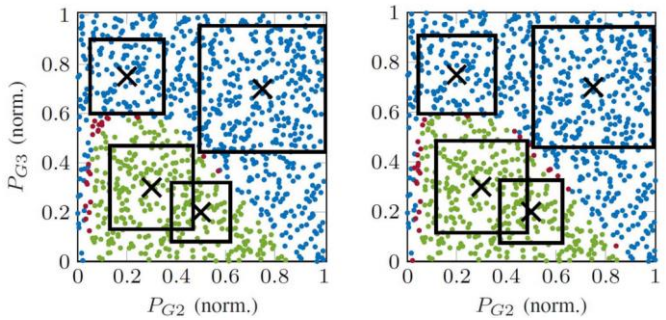
$$\max_{x \in \mathcal{X}} \|\mathbf{physics}(x) - \mathbf{ML}(x)\|$$

We thus have a **unique** opportunity to compare ML model predictions to the ground-truth physics (directly, or indirectly)

- *Solution gives a performance guarantee*
- There is no analog in many other ML applications, e.g., image classification models have no first-principles comparison

Verification in Power Systems — A 6-Paper Journey

1. Verification of NN behavior: Formal guarantees for power system applications
   - (Venzke, Chatzi., TSG'20): Trained NNs to predict regions of small signal/N-1 stability



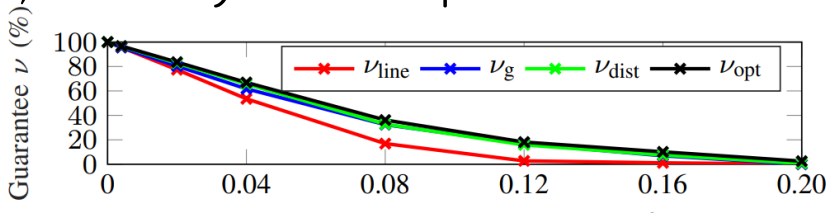
$$\min_{\mathbf{x},\hat{\mathbf{z}},\mathbf{z},\mathbf{y},\epsilon} \quad \epsilon \qquad (10a)$$

$$\text{s.t.} \quad (2),\ (3),\ (8a)-(8e) \qquad (10b)$$

correct safe · correct unsafe · misclassified · verification samples

Regression Error

2. Learning Optimal Power Flow: Worst-Case Guarantees for Neural Networks
   - (Venzke, Qu, Low, Chatzi., SGC'20): Verified performance of NN-based DCOPF solvers



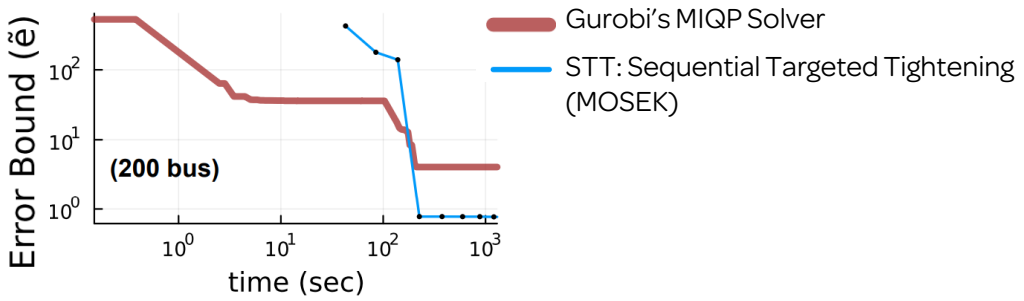
Nonlinearity

3. Physics-Informed Neural Networks for AC Optimal Power Flow
   - (Nellikkath, Chatzi., PSCC'22): Worst-case performance of NN-based ACOPF solvers
     - » *"We were unable to compute the worst-case line flow constraint violation since the MIQCQP problem could not be solved to zero optimality gap within 5 hr."*

Scale (Bounds)

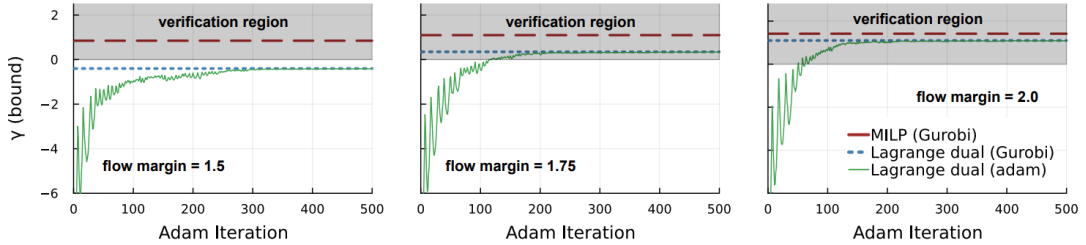
Verification in Power Systems – Key Papers

4. Global Performance Guarantees for Neural Network Models of AC Power Flow
   - (Chevalier, Chatzi., submitted '24): Targeted SDP cuts to enhance solver scalability



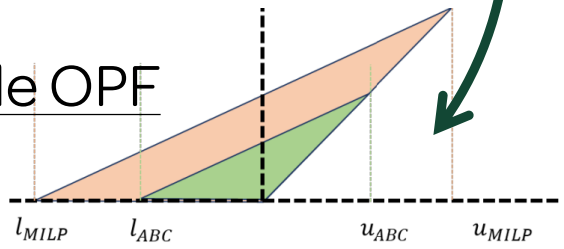
GPUs

5. GPU-Accelerated Verification of Machine Learning Models for Power Systems
   - (Chevalier, Murzakhanov, Chatzi., HICSS'24): Exploited GPU-based tools from ML community



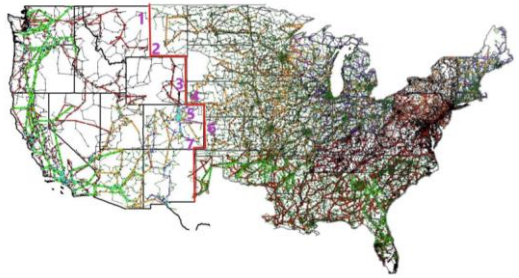
GPU + CPU

6. Scalable Exact Verification of Optimization Proxies for Large-Scale OPF
   - (Nellikkath, et al, Van Hentenryck, submitted '24): GPU-based tools to accelerate MILP convergence on CPU-based Gurobi

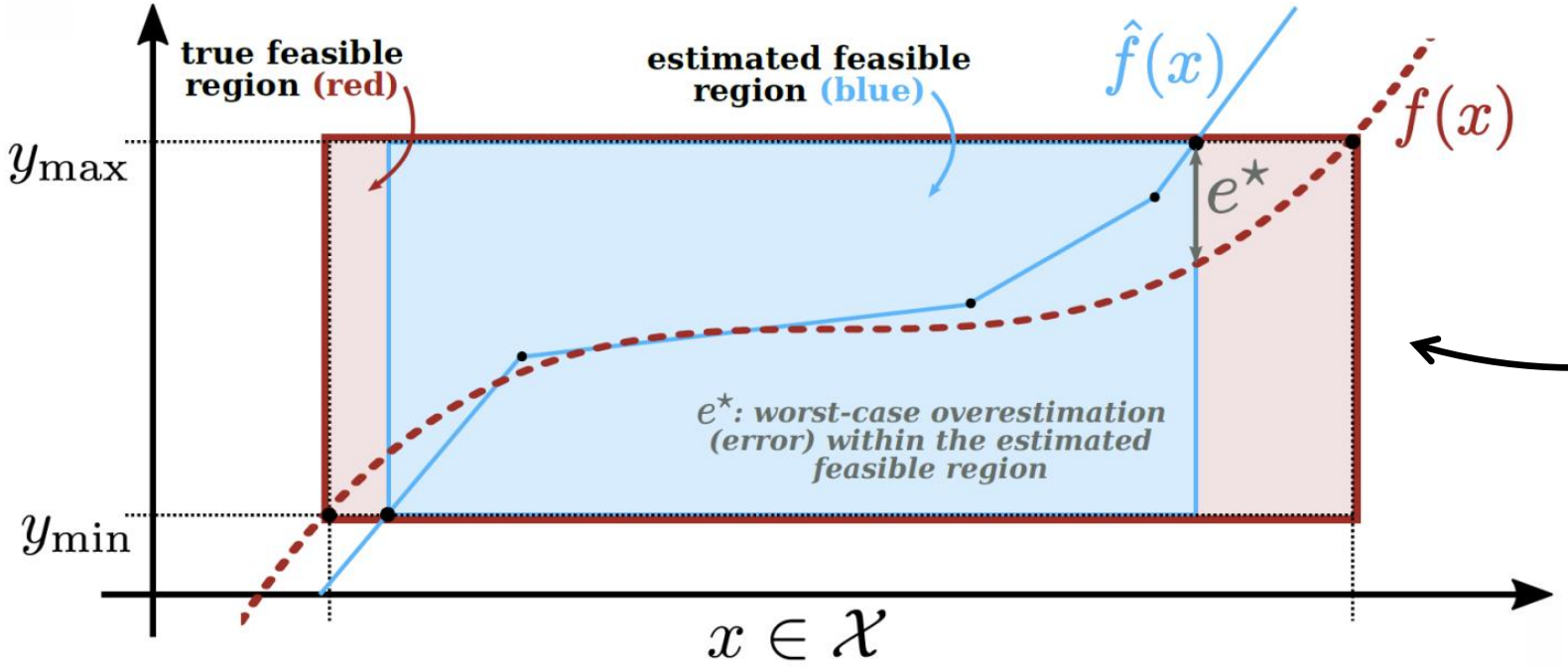


Paper: Global Performance Guarantees for NN Models of AC Power Flow

- Consider a NN power flow mapping: $\hat{f}(\underbrace{v_r, v_i}_{x}) \rightarrow (\underbrace{\mathrm{V}^2, p^{\mathrm{inj}}, q^{\mathrm{inj}}, l^{\mathrm{ft}}, l^{\mathrm{tf}}}_{y})$



- In our paper, we ask, "What is **the worst case performance** of a NN surrogate model relative to the ground truth?"



Quadratic (power)

$$e_i^\star = \max \; f_i(x) - \hat{f}_i(x)$$
$$\text{s.t.} \; \hat{f}(x) \geq 0$$

MILP (NN)

Paper: Global Performance Guarantees for NN Models of AC Power Flow

$$
\begin{aligned}
e_i^\star = \max_x \quad & x^T \boldsymbol{M}_i x - c_i^T x \\
\text{s.t.} \quad & \boldsymbol{A}x - b \geq 0 \\
& x_b \in \{0,1\}^d
\end{aligned}
$$

Nonconvex MIQP (Gurobi)

Double **Semidefinite Programming (SDP) Relaxation (binaries and quadratic terms!)**

$$
\begin{aligned}
e_i^\star \leq \max_x \quad & \mathrm{tr}(\boldsymbol{M}_i \boldsymbol{X}) - c_i^T x \\
\text{s.t.} \quad & \boldsymbol{A}x - b \geq 0 \\
& (\boldsymbol{A}\boldsymbol{X}\boldsymbol{A}^T - \boldsymbol{A}xb^T - (\boldsymbol{A}x)^T b + bb^T \geq 0)_i,\ i \in \mathcal{S}_c \\
& \begin{bmatrix} 1 & x^T \\ x & \boldsymbol{X} \end{bmatrix} \succeq 0
\end{aligned}
$$

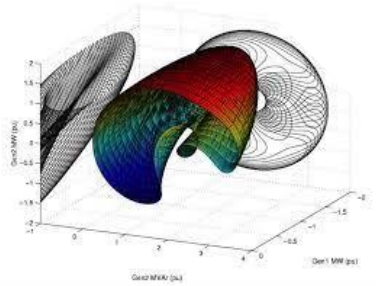
Convex SDP (MOSEK)

- **Tighten relaxation with "RLT" cuts! Only a few are needed, it turns out (which?)**

$$(\boldsymbol{A}x - b)(\boldsymbol{A}x - b)^T = \boldsymbol{A}\underbrace{xx^T}_{\boldsymbol{X}}\boldsymbol{A}^T - \boldsymbol{A}xb^T - (\boldsymbol{A}x)^T b + bb^T \geq 0$$

Paper: GPU-Accelerated Verification of ML Models for Power Systems

- In power systems, many ML models will need to be constrained to obey (not satisfy, per se) grid physics
  - Example: DERs in a distribution grid: they make a control decision, and voltages react, but reaction lives on a manifold



$$\gamma = \min_{x,y,z} \quad c^T z$$
$$\text{s.t.} \quad y = \text{NN}(x)$$
$$Ay = z \ : \ \lambda$$
$$Bz \leq h \ : \ \mu,$$

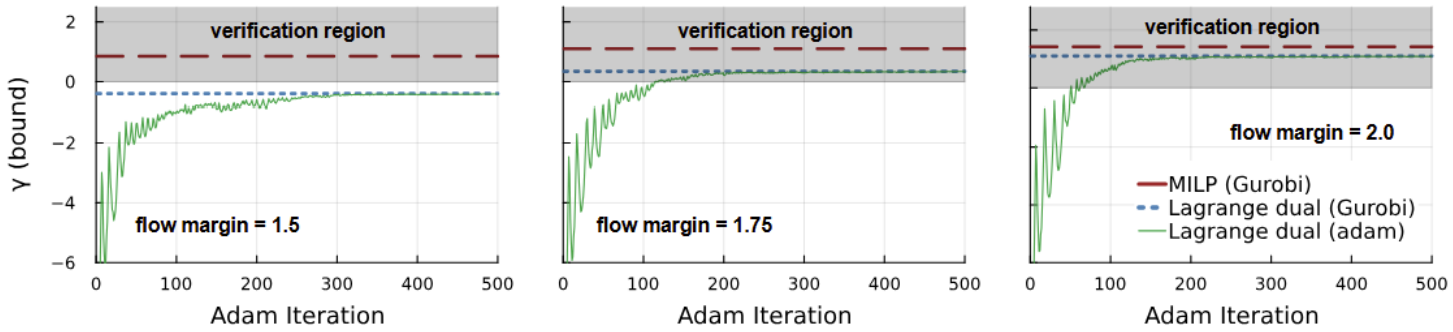
Dualize network physics

$$\gamma = \max_{\mu \geq 0, \lambda} \min_{x,y,z} \quad \lambda^T A y + (c + B^T \mu - \lambda)^T z - \mu^T h$$
$$\text{s.t.} \quad y = \text{NN}(x).$$

Now, apply class tricks to solve this ☺

ECE598HZ: you all have pretty good tools for dealing with this part!!!

AB-CROWN, AutoLirpa, etc…



Lecture (Talk?) Outline

①

Challenges

...in actual, and future, power systems.

②

Tools

...for overcoming these challenges (ML + verification)

③

Synergies

...between ML verification and grid operation.

Synergies: Grid Operation and ML Verification

& Problems...

Power System Operation and ML Verification are both "MINLPs"

Power Grid Operation

- Network is **sparse**
- Highly structured (**physics**)
- Dominated by binaries and bilinearities
- Local optimality is ok, but need primal feasibility
- Similar problems solved over and over and over on same network

ML Verification

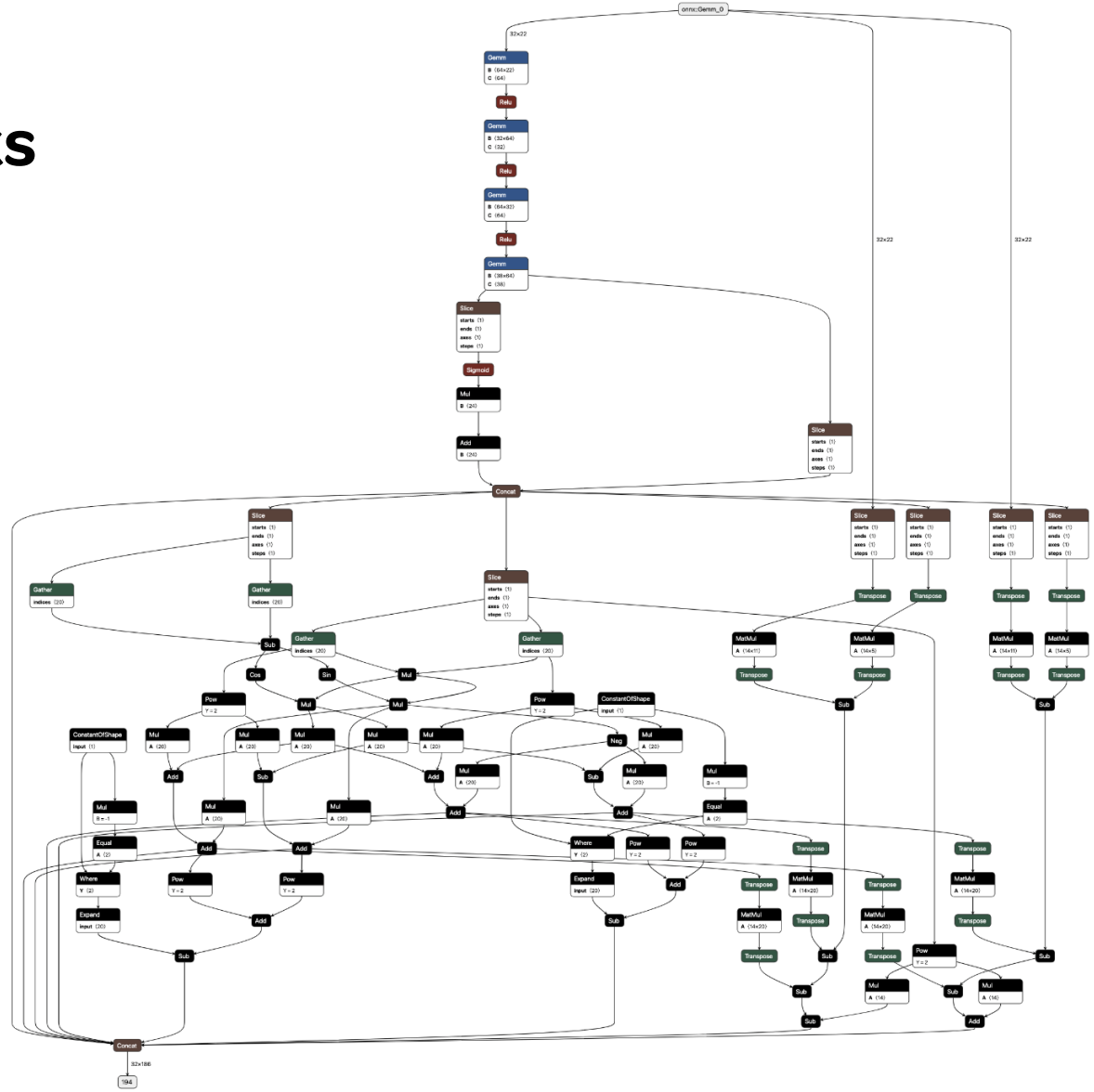
- Network is generally **dense**
- Highly structured (eg, **forward pass**)
- Dominated by binaries and many types of nonlinearities
- Need a global bound, or a local adversarial perturbation
- Similar problems solved on perturbed network (i.e., after retraining)

Synergy I: Computational Graphs

Both power grids and Neural Networks are computational graphs!

This is the “ML4ACOPF” NN, which is a VNNComp benchmark network:

- It takes a power system load, predicts an Optimal Power Flow solution, and then uses direct calculation to infer if the solution violates any constraints
- A verifier can then “search” for a loading condition which leads to violation.
- First half of the network is ML (dense); second half is sparse (physics)



Synergy I: Computational Graphs

Problem: Forward Pass in a Grid…?

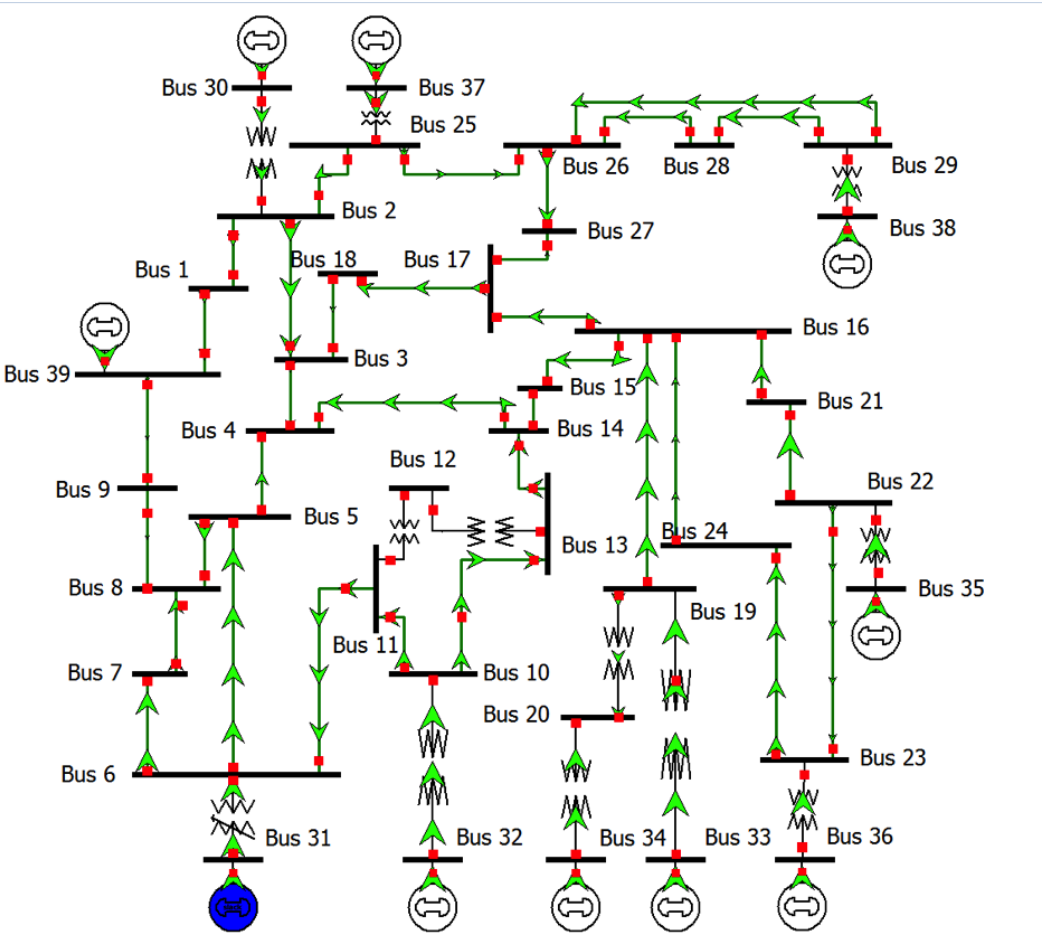
Unlike a NN, the definition of a "forward pass" is not obviously defined in a power grid

Nodal voltages cause currents to flow, engendering power flow injections.

One option:

- given V, compute the rest (**forward pass**)
- given the rest, compute V (**backward pass**)

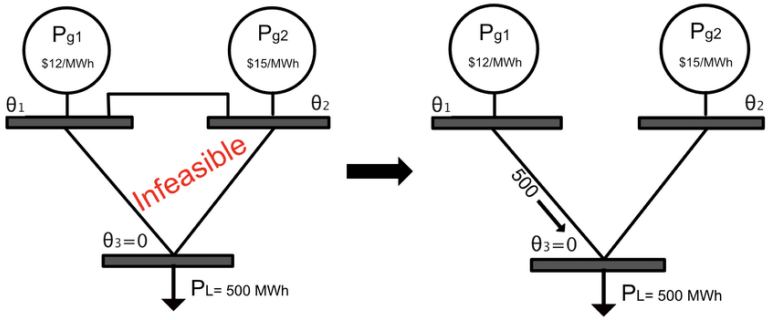
Do you have a better idea? Awesome implications, if so (next slides…)



Synergy II: Both "Need" Branch-and-Bound Solvers

Electric Power Grids

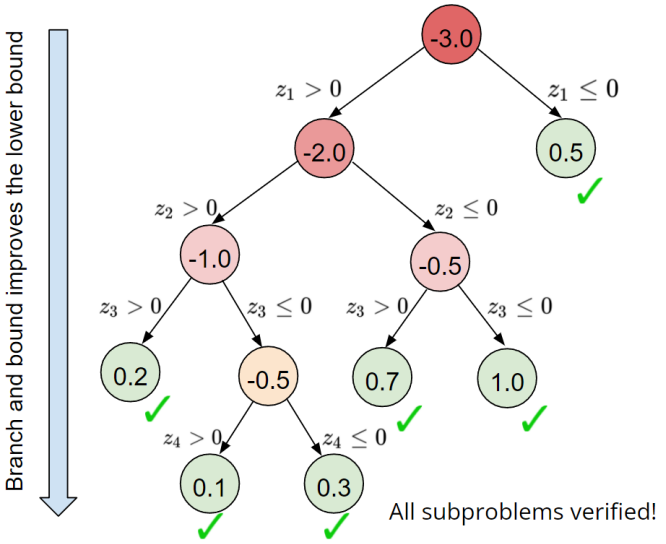
- Used to switch transmission lines, turn generators on/off, switch voltage controllers, branch over bilinear nonconvexities, etc.
- DOMINATES industry (MISO, ERCOT, ISO-NE etc)



Crozier

ML Verification

- Used to toggle activation functions on and off, in search of a lower bound (or, to find better adversarial inputs to the model)



Synergy II: Both "Need" Branch-and-Bound Solvers

- α,β-CROWN's amazing gradient-based, dual-formulated B&B performance directly inspired "**QuasiGrad**", the solver I built to compete in the GO competition

A Parallelized, Adam-Based Solver for Reserve and Security Constrained AC Unit Commitment

While Adam has been a successful tool for solving large-scale nonlinear programming (NLP) problems, it has also recently been used to solve sub-problems in massive Mixed-Integer Linear Programming (MILP) Branch-and-Bound (BaB) problems. The α, β-CROWN solver [7], which has won the most recent International Verification of Neural Networks Competitions (VNN-COMPs) [8], uses a GPU-accelerated Adam solver to verify the performance of ex-

Rank	Team	Division 2 Score	$k
	Ensemble	**163,579,841,300**	
1	GOT-BSI-OPF	162,941,475,726	100
2	TIM-GO	162,270,256,651	90
3	YongOptimization	160,165,088,341	80
4	Artelys_Columbia	157,359,267,058	70
5	GravityX	156,131,225,903	60
	ARPA-e Benchmark	156,014,230,887	
	quasiGrad	155,168,735,676	
	Occams razor	145,494,618,835	
	Electric-Stampede	139,357,283,507	
	LLGoMax	116,812,192,654	
	The Blackouts	114,098,832,983	
	Gatorgar	10,263,109,863	

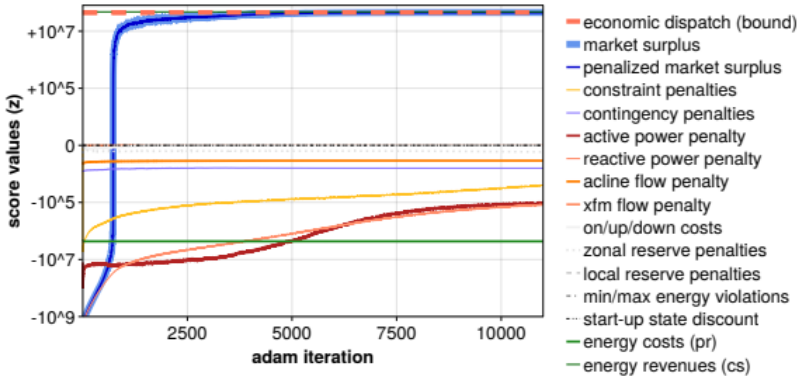


Fig. 1: Illustrated is an Adam solve on a 617-bus, 18 time period, real-time market clearing test case (integers relaxed); this system is initialized with a copper pate economic dispatch solution (LP), whose upper bound is given as the orange dashed line. Within several thousand iterations, Adam finds an AC network solution to within 1% of this global bound. A single back-propagation (i.e., gradient calculation) through this entire system, include all 18×562 contingencies, takes ~24ms when parallelized on 6 CPU threads.

- Results were very mixed, but I did solve power systems with **100 million+ variables**

Synergy II: Both "Need" Branch-and-Bound Solvers

The QuasiGrad approach has 2 general problems:

- **Problem I: Termination.**
  - ML verification B&B terminates when (i) a lower bound is proved >0, or (ii) an adversarial input is identified
  - Power system B&B terminates when the **global optimality** is reached: ***way harder***

- **Problem II: Nonlinearity (switches!!)**
  - Integers in power systems generally represent discontinuous switches, while ReLUs are continuous

Synergy III: Both Seek to Protect Against Adversarial Attacks

Electric Power Grids

- Specifically **enumerates** "contingencies" and finds a single operating point which guards against all of them
- Grid operators may utilize:
  - "**security constraints**" to guard against network component (line) loss
  - "**reserve constraints**" to ensure enough spinning reserve, etc, in grid zones
  - "**chance constraints**" to guard against probabilistic overloading or renewables

ML Verification

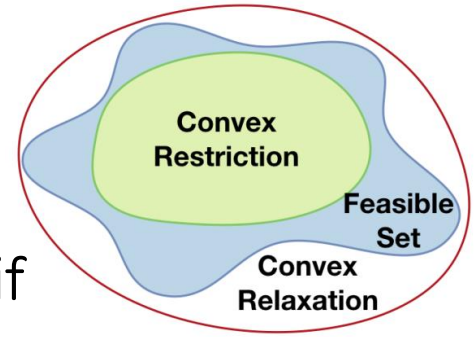
- Given a model that "does something", verification typically searches for a conceivable violation of some metric
- These violations may include:
  - Adversarial perturbations
  - Correctness violation
  - Lack of monotonicity or
  - Violation of terms of constraints

Searches for working operating point in an apriori broken model ⟷ **Searches for broken operating point in an apriori working model**

Synergy IV: Convex Restrictions Can be Useful!

Electric Power Grids

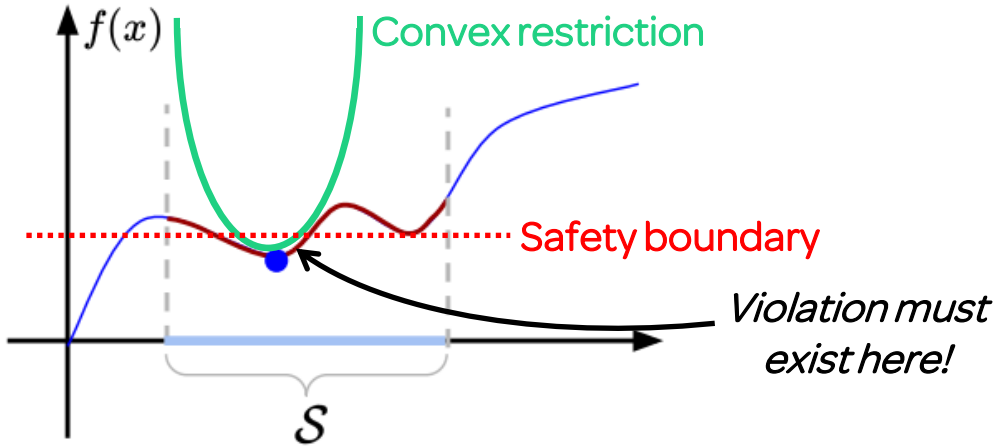
- Convex restrictions can guarantee the existence of a "robust" solution within some operational space [1]
- Fixed point theorems (e.g., Browers) can guarantee that, under some bounded perturbation, a **feasible solution will still exist**, even if we don't explicitly find it



Proves the existence of something good.

ML Verification

- Convex restrictions can guarantee the existence of an adversarial input, even if we never actually find it – useful?



Proves the existence of something bad.

[1] D. Lee, H. D. Nguyen, K. Dvijotham and K. Turitsyn, "Convex Restriction of Power Flow Feasibility Sets," in *IEEE TCNS*, Sept. 2019.

Synergy V: Bounding of Nonlinearities

Electric Power Grids

- Can we tighten over power system nonlinearities? How about **bilinearity**?

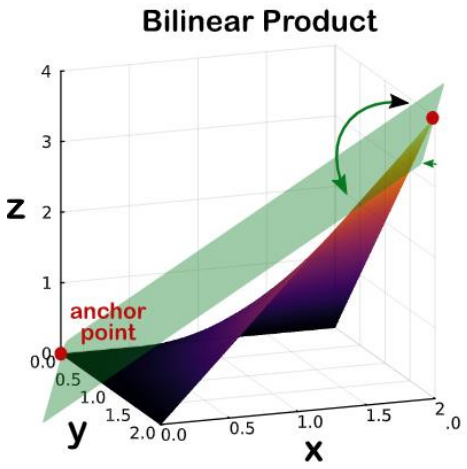
$$z \triangleq xy = \alpha_1 x + \alpha_2 y + \beta$$

$$\alpha_1 = y$$

$$\alpha_2 = x$$

$$\underbrace{\beta = -\alpha_1 \alpha_2}$$

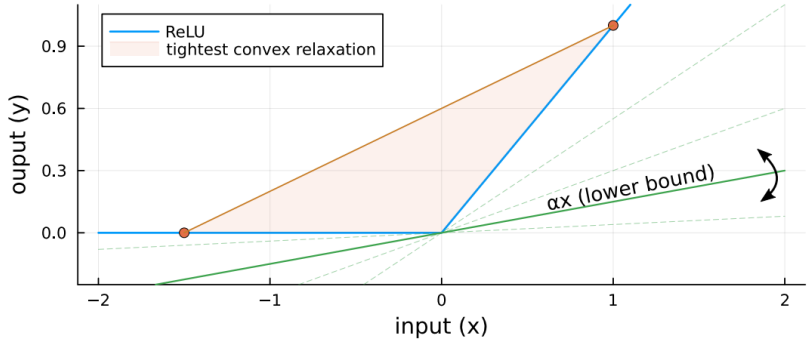
$$z = \alpha_1 x + \alpha_2 y - \alpha_1 \alpha_2$$



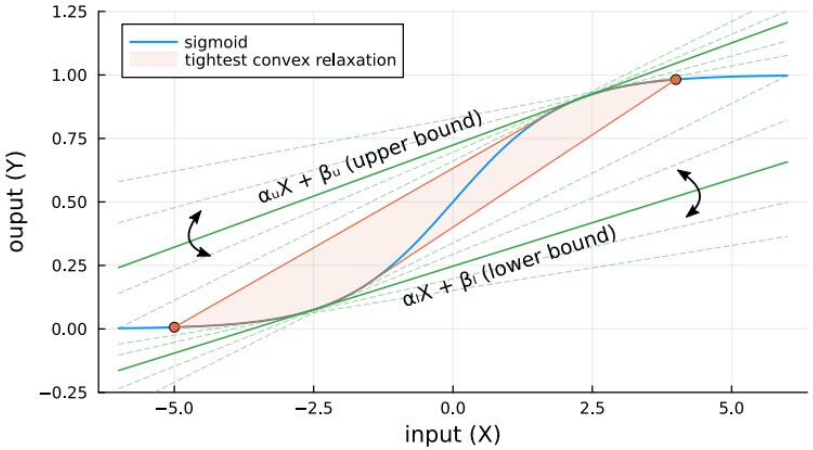
Problem: convexifying ugly non-convexitites in power systems pushes you far from feasibility

ML Verification

- Tighten over ReLUS via α-CROWN:



- Tighten over sigmoid via α-sig:



Synergy VI: Find Intermediate Bounds! ❤

Electric Power Grids

- Bounding intermediate variables in a big problem has huge benefits
  - **Big-M** values in MILP optimization,
  - Upper/lower bounds in bilinear McCormick **envelopes**,
  - Sequential/optimization-based bound tightening (OBBT) for state estimation and global opt.
  - Faster B&B tree trimming, even
- Power system researchers are historically clever, but technologically constrained on this task (**no GPUs**!)

ML Verification

- Auto-LiRPA is **very good** at this sort of thing. However, it isn't 1:1 applicable to bounding variable in the problem

$$\begin{aligned} &\min\ c(x) \\ &\text{s.t. } f(x) = 0 \\ &\quad\ g(x) \leq 0 \end{aligned}$$

- General Cutting Plane (GCP-CROWN) is a step in the right direction...
- ...but **INVPROP** is a game changer

Synergy VI: Find Intermediate Bounds! ❤

Let's assume you **don't know** good bounds on the input (e.g., voltage)

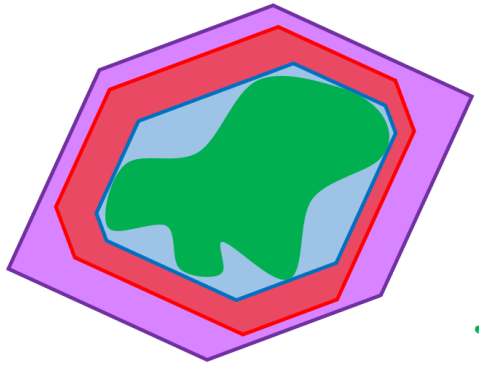
- Can you take an output bound and propagate backwards to the input?
  - **Sure!** Just use INVPROP [1].

Bounded Input (Conventional)

$$\min_{x \in \mathcal{S}_{\text{in}}} \; c^T y$$
$$\text{s.t. } y = \text{NN}(x)$$

Bounded Output (INVPROP)

$$\min_{x} \; c^T x$$
$$\text{s.t. } \text{NN}(x) \in \mathcal{S}_{\text{out}}$$



$$\mathcal{S}_{\text{over}} \supseteq$$
$$\mathcal{S}_{\text{LP}} \supseteq$$
$$\mathcal{S}_{\text{MILP}} \supseteq$$
$$f^{-1}(\mathcal{S}_{\text{out}})$$

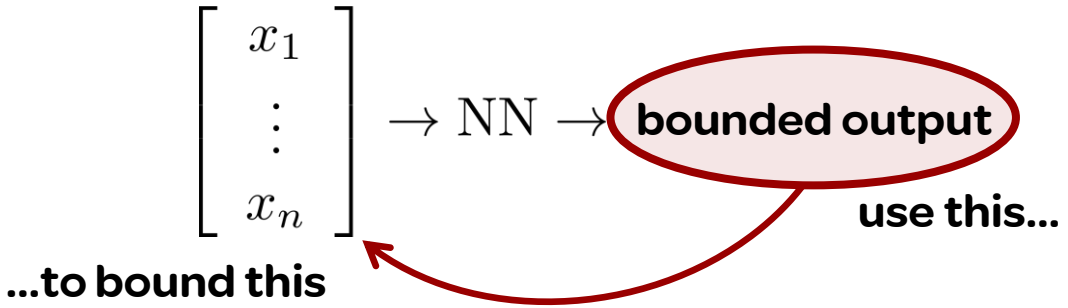
  - **Most exciting:** you can bound any input, or any arbitrary cut!

[1] Kotha, Suhas, et al. "Provably bounding neural network preimages." *NeurIPS* (2024).

Synergy VI: Find Intermediate Bounds! ❤

Most exciting: you can bound any input, or any arbitrary cut!

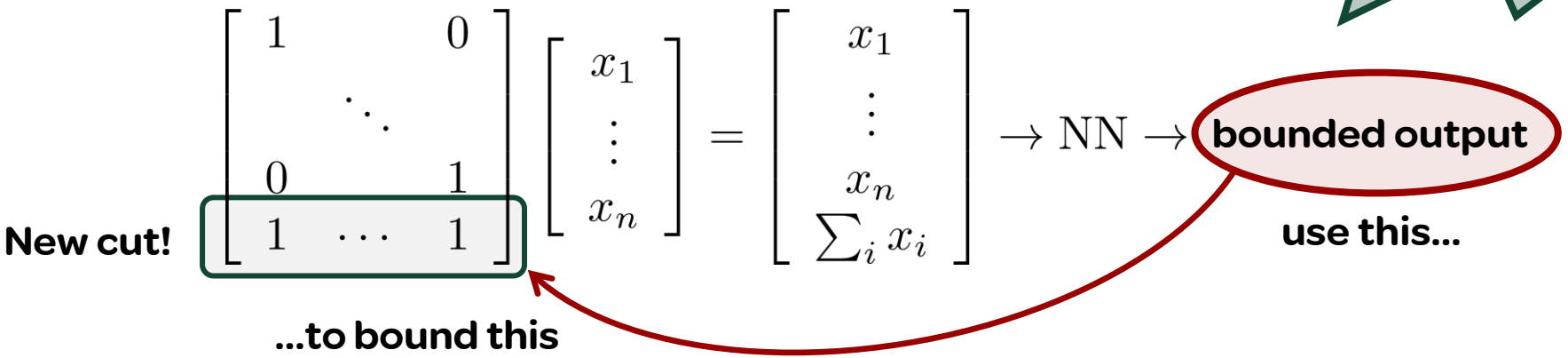
1. Direct bounding of inputs:



Potential (Non-ML) Uses

McCormick Bounds
Big-M Tightening
Reachability Analysis
Feasibility Tests...

2. Bounding of new, useful **cuts**!



1. Trained NN to emulate DC-OPF

$$\mathrm{NN}(p_d) \rightarrow p_g$$

2. Given output generation limits:

$$\underline{p}_g \leq p_g \leq \overline{p}_g$$

↓

INVPROP

↓

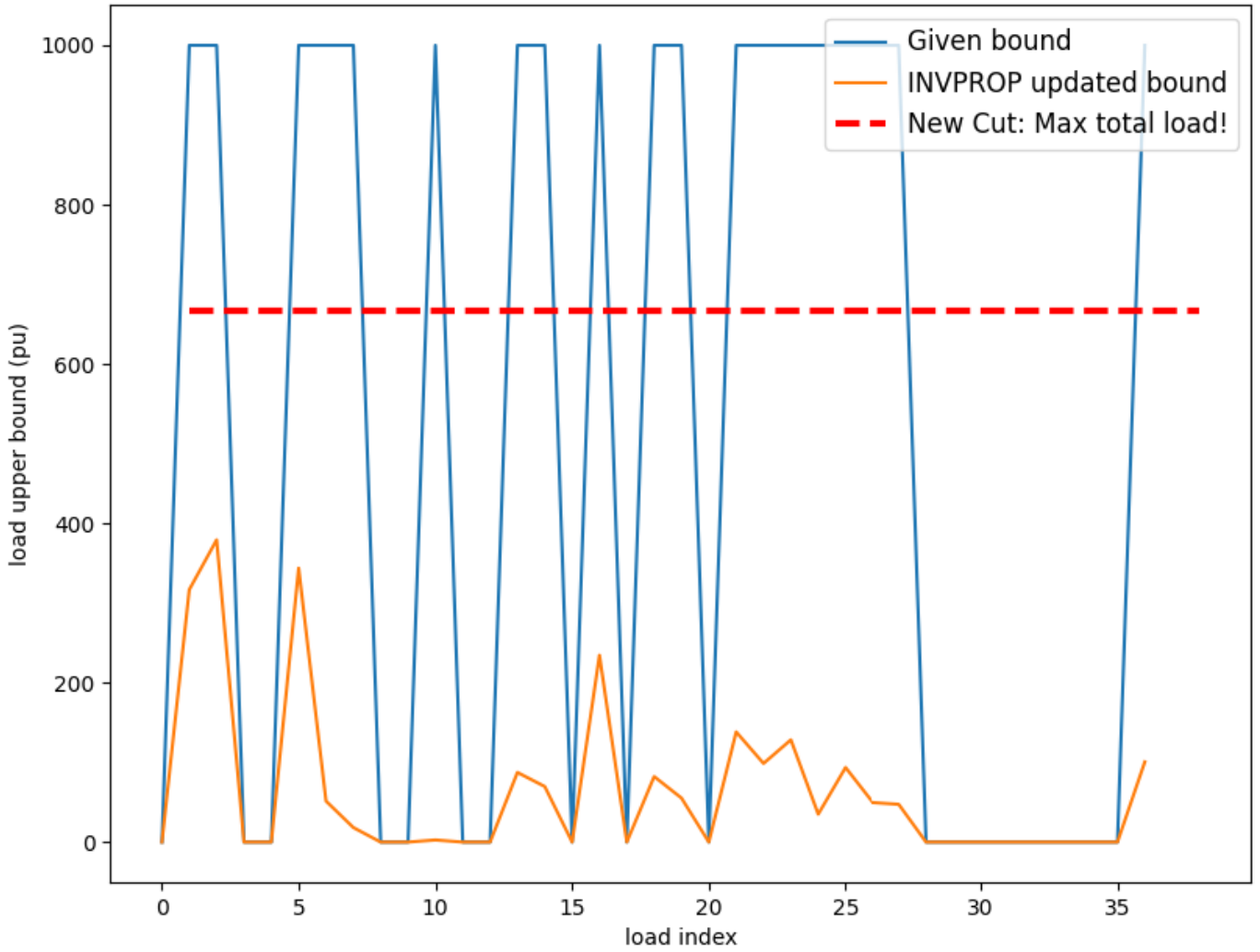
Improved blue bound to orange bound (load inputs)!

3. I then asked INVPROP to compute a new cut:

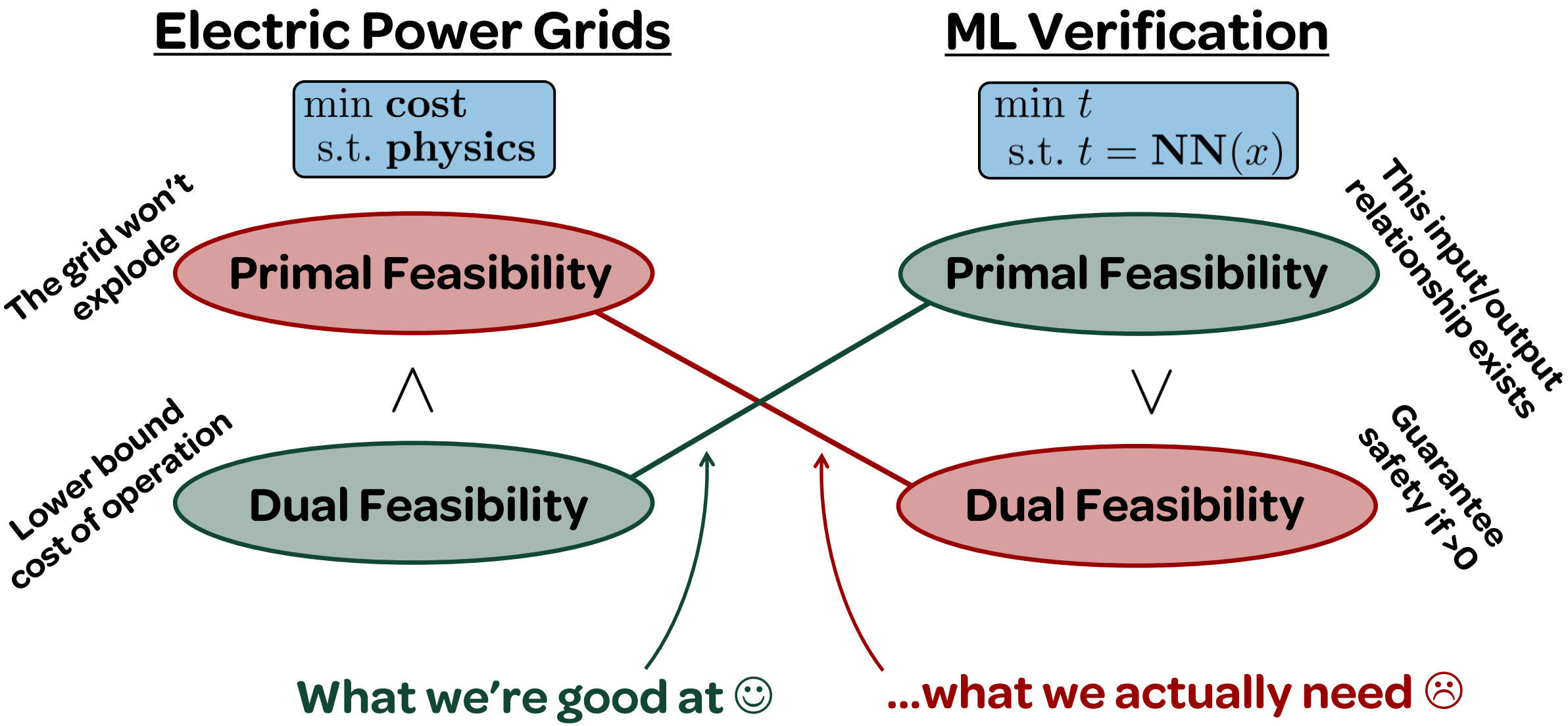
$$\sum p_d \leq ?$$

↓

Red bound! (3x+ tighter than just $\sum$[orange bound])



(Anti?)Synergies: Grid Operation and ML Verification



Summary

- Neural Network verification is a hard, **NP-complete** problem
- Power grid reliability/security is also **NP-compete**, in the sense that a potential solution is checkable in polynomial time
- Grid **optimization**, however, is generally **not in NP**, because we want a solution which is "globally optimal" and secure
  – If a solution is not optimal, market participants may **not be happy**…

- If ML is embraced by system operators, we will want guarantees that it is **reliable** (NP-complete) and, in some many, **optimal** (not in NP)
- Verification and grid optimization share many exciting congruent + dual characteristics, and the **future is bright**

- Finally, if you want to **work on these problems**…

Come to Vermont!

(For a PhD)

NEST-VT

CREATE