# Harnessing Simulated Datasets with Graphs:

## Thesis Dissertation Proposal

Henrique Teles Maia

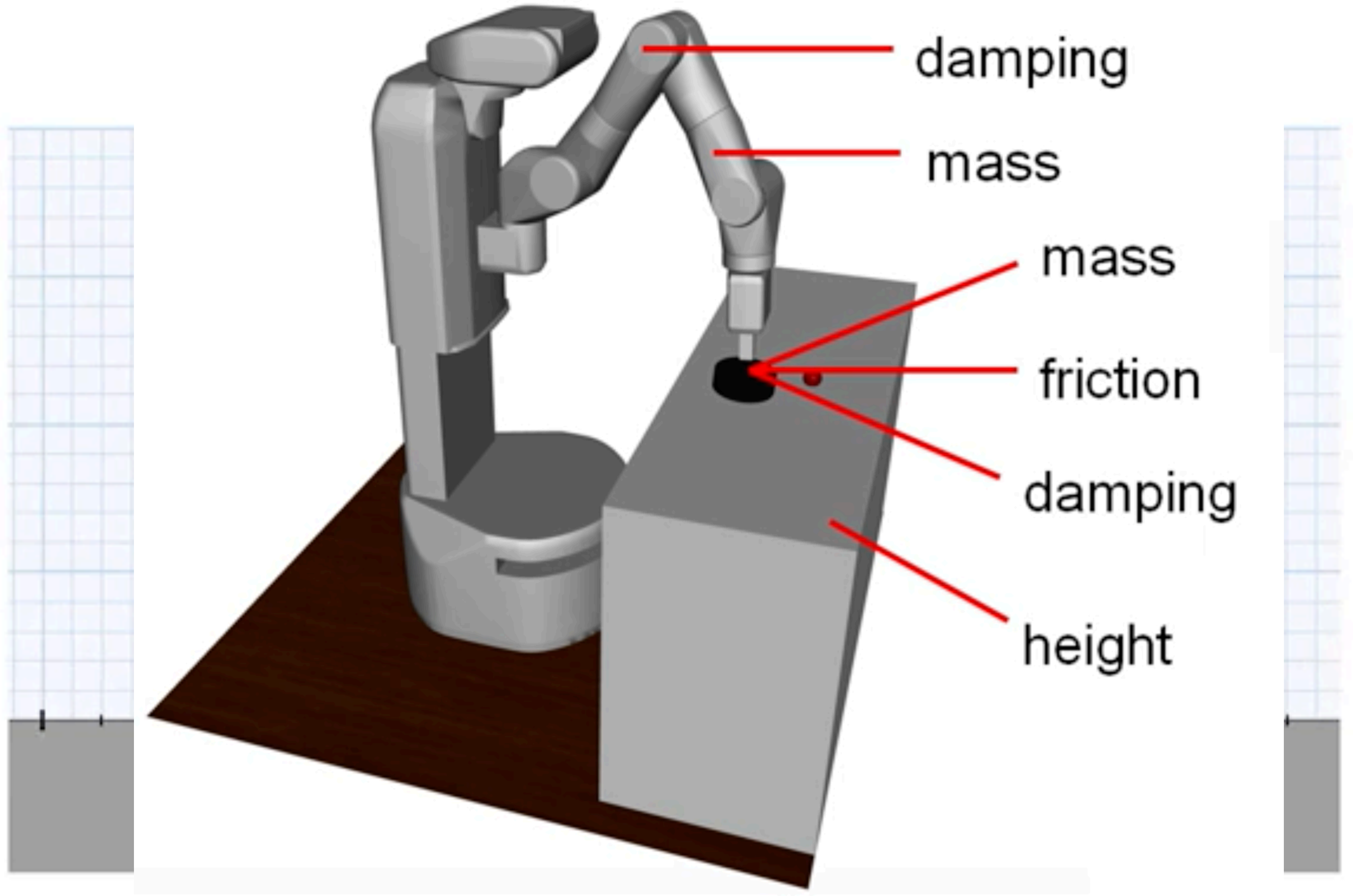
Columbia University
in the City of New York

# Modeling Realistic Behavior


DeepMimic
[Peng et al. 2018]

Using Deep Convolutional Neural Networks
[Laine et al. 2017]

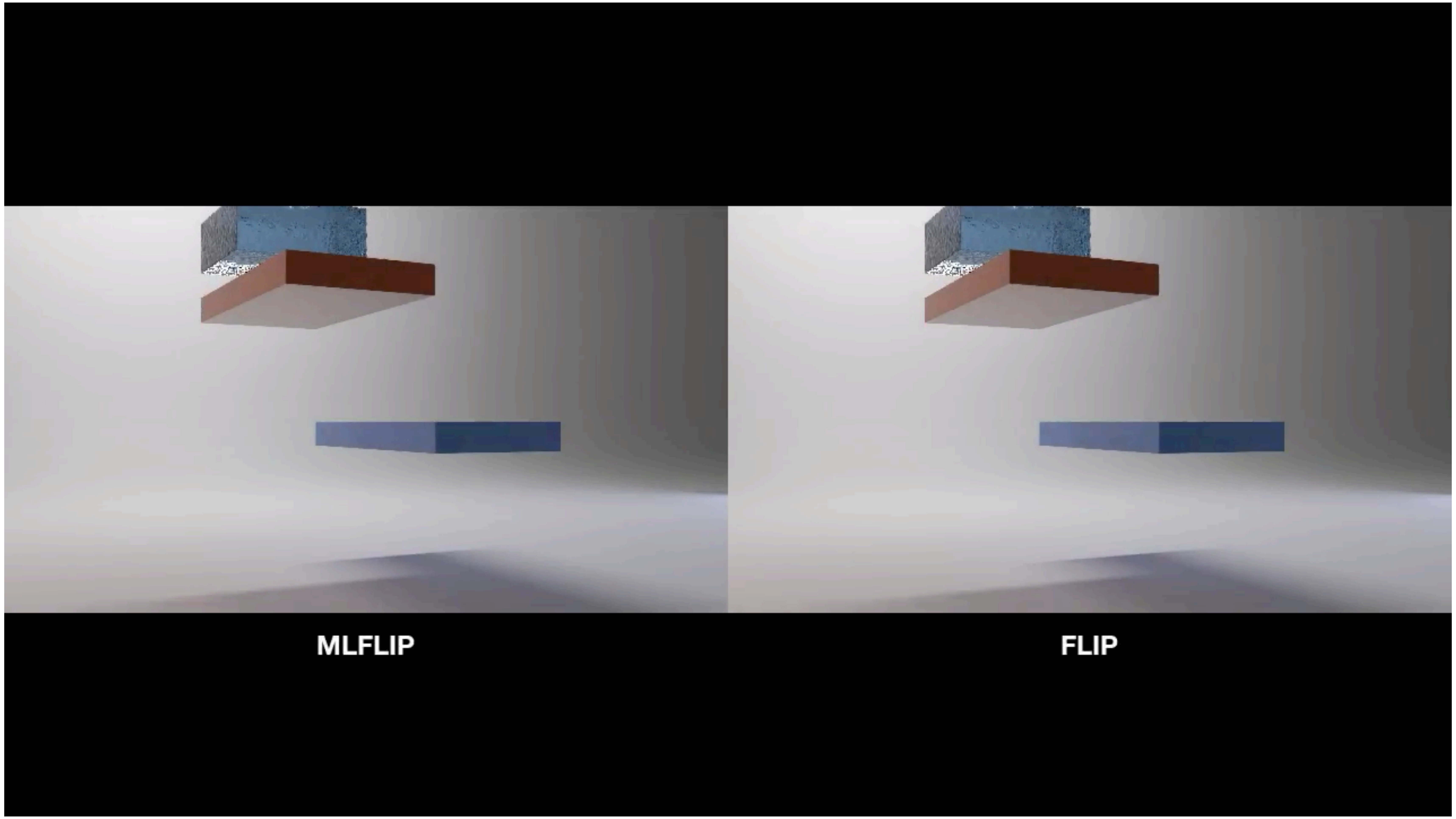
# Simulated data




Sim-to-Real Transfer of Robotic Control
with Dynamics Randomization
[Peng et al. 2018]

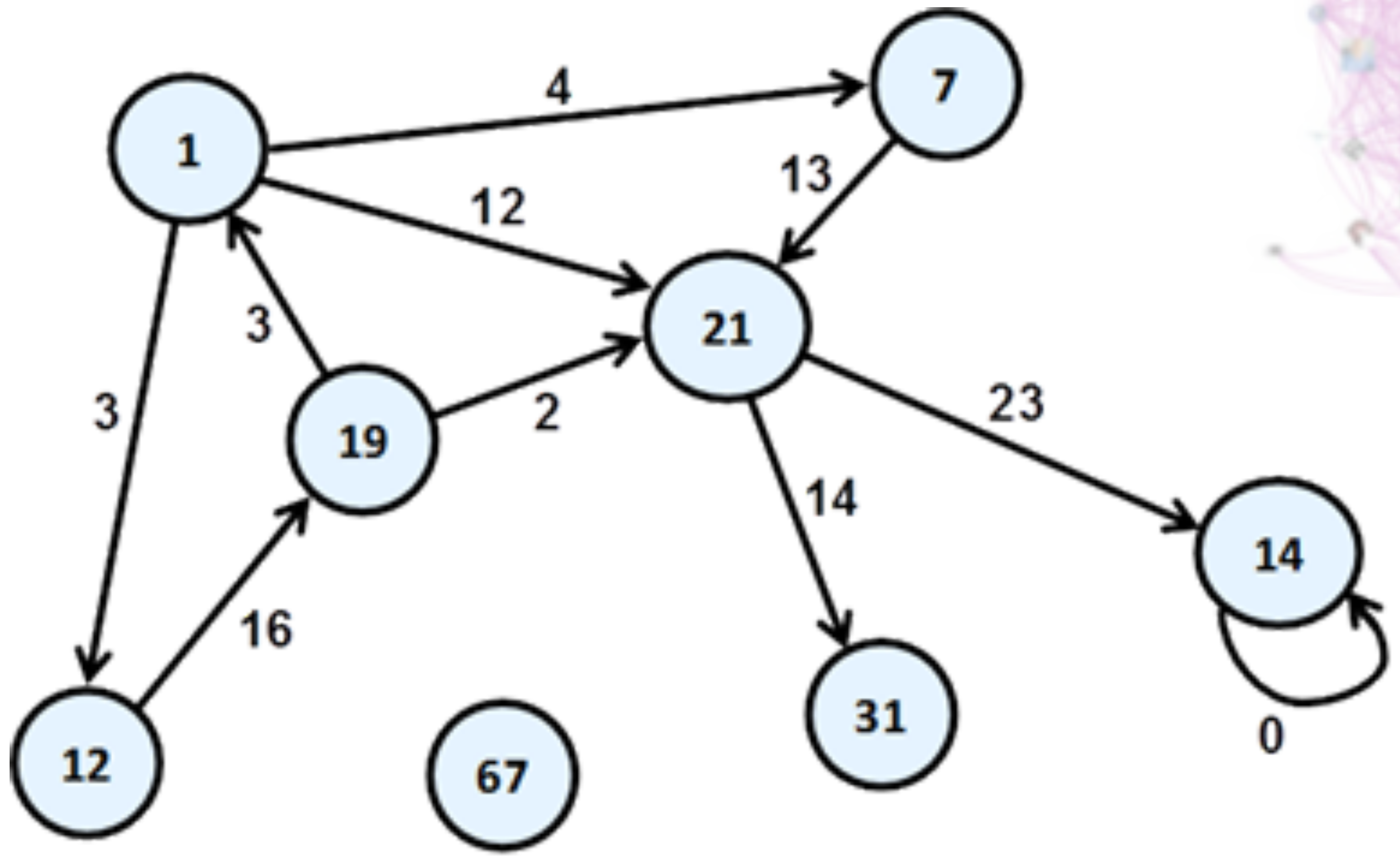
Dynamic Terrain Traversal Skills
Using Reinforcement Learning
[Peng et al. 2015]

# Combinatorial Explosion

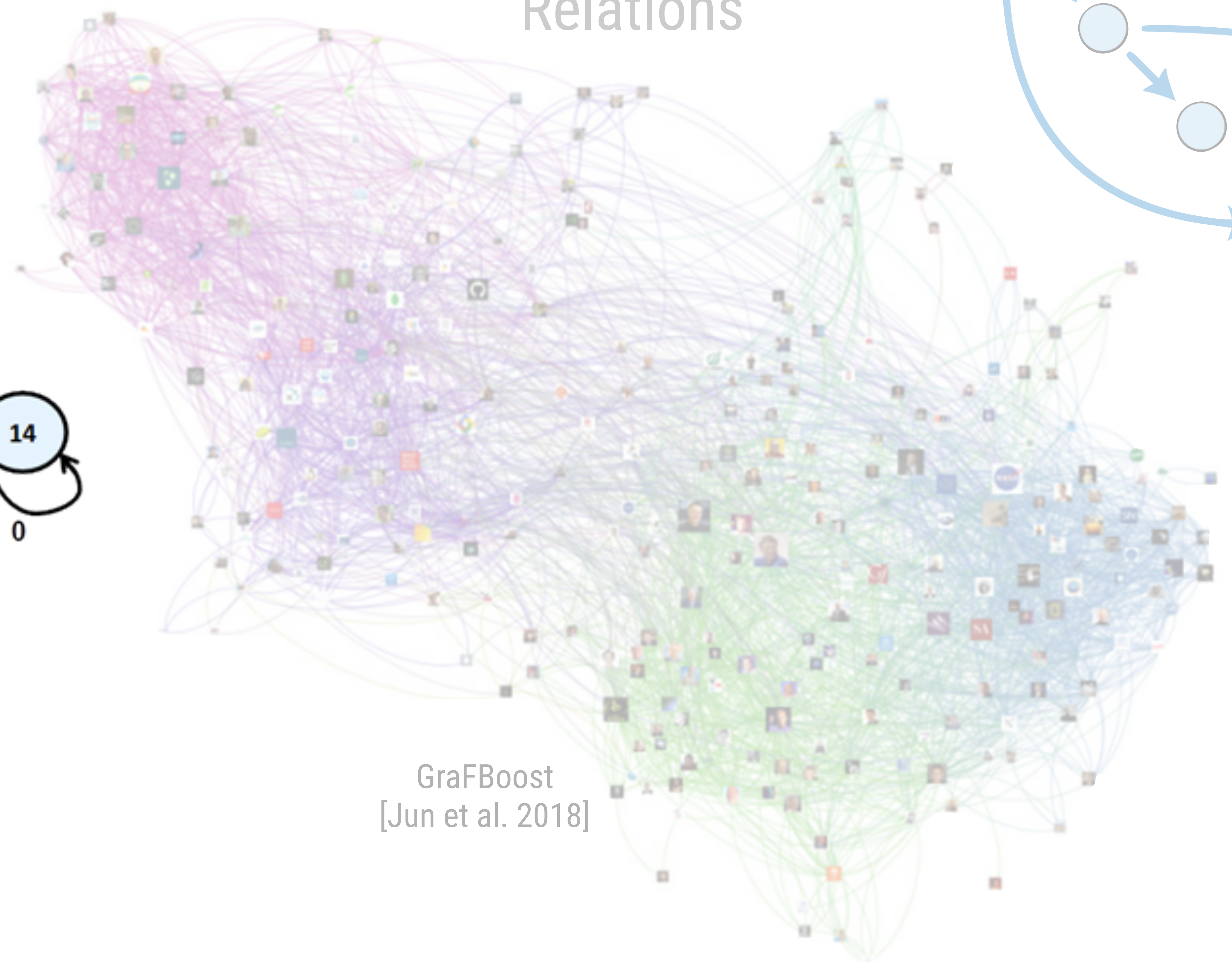



Liquid Splash Modeling
with Neural Networks
[Um et al. 2018]

# Graphs




Pairwise
Dependencies



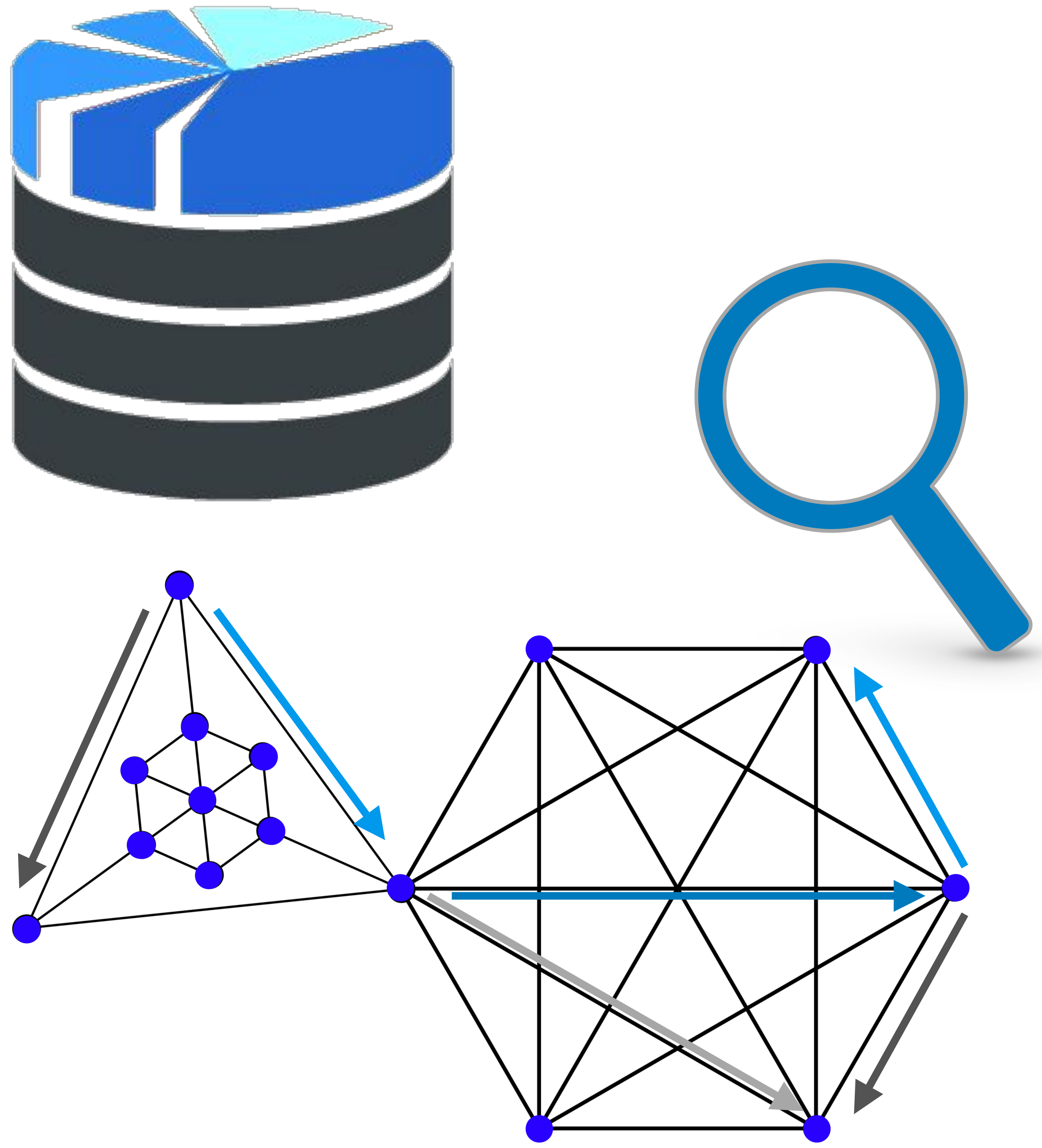
Semantic
Relations

GraFBoost
[Jun et al. 2018]

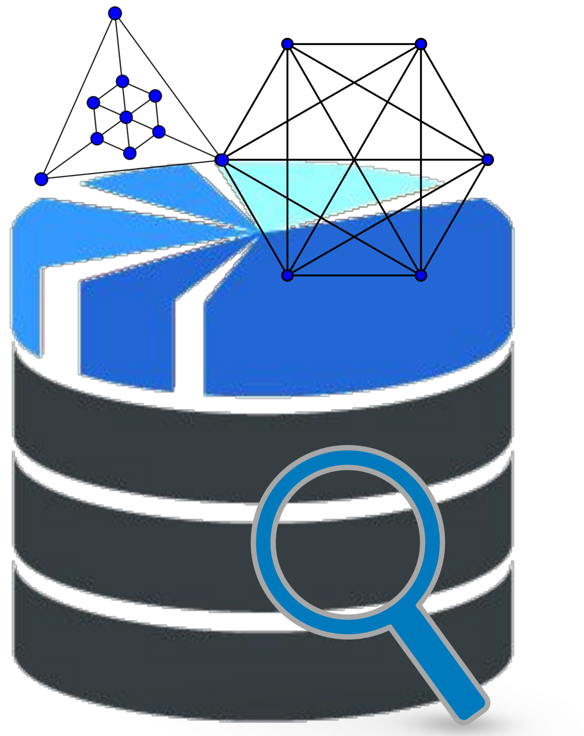
Topological
Orderings

# Methodology

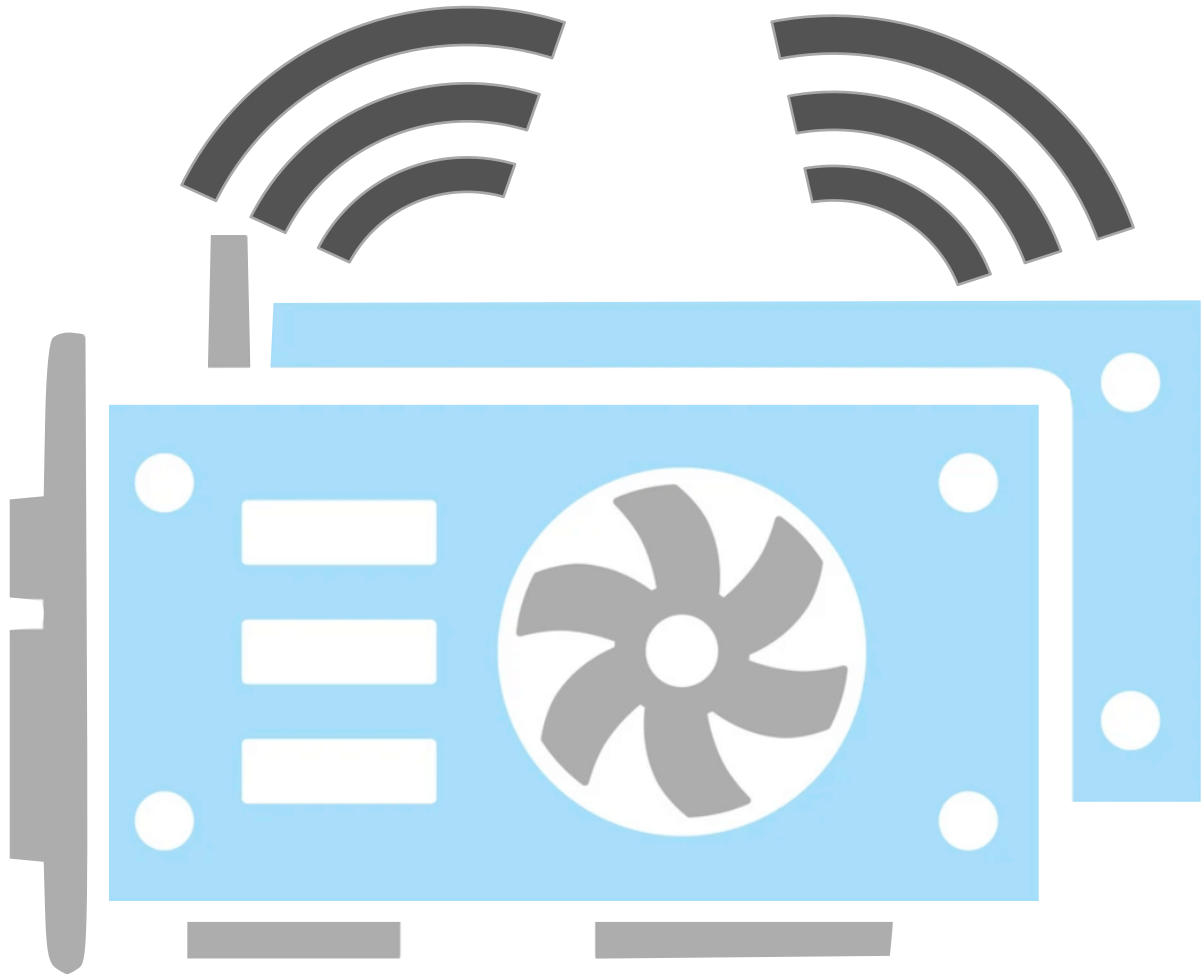
- ➡Generate a specialized dataset
- ➡Identify combinatorial challenges
- ➡Overlay a graph structure
- ➡Leverage graph algorithms



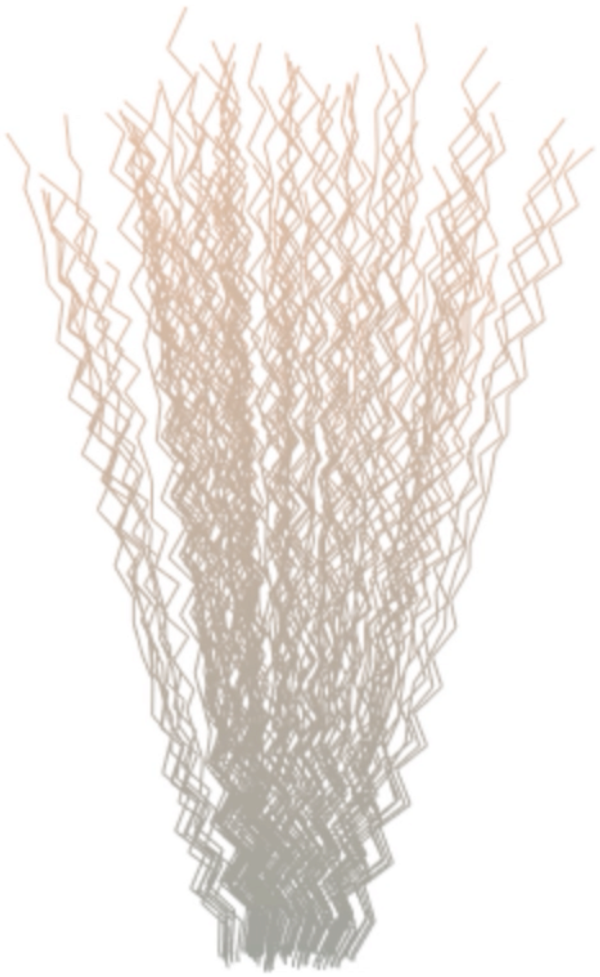
# Roadmap



Additive Manufacturing



Side-channel Security



Physics-based Contact

# LayerCode:
## Optical Barcodes for 3D Printed Shapes

with Dingzeyu Li, Yuan Yang, Changxi Zheng

COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Adobe

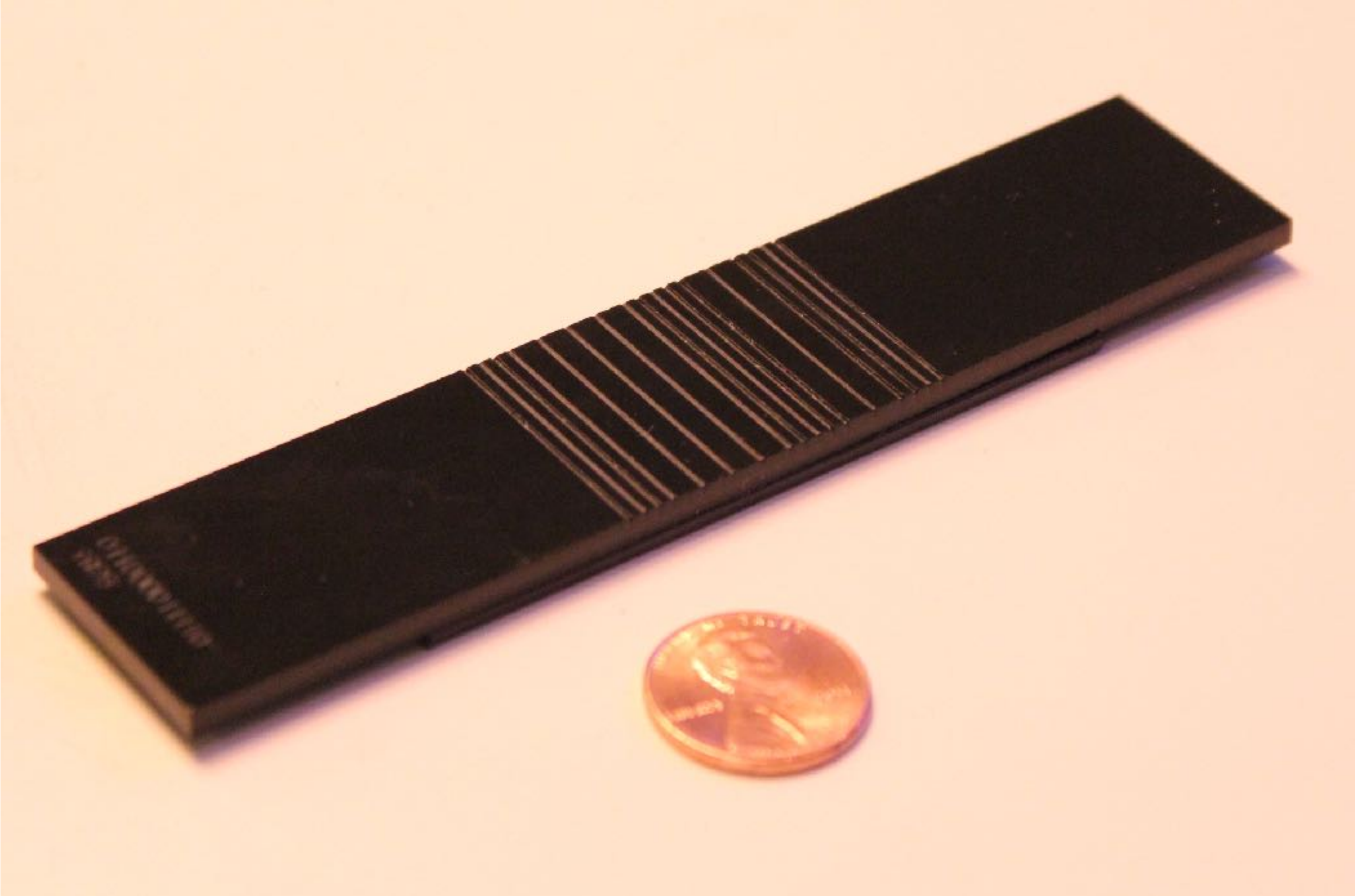
# 2D Tagging


BOARDING PASS
PASSENGER TICKET AND BAGGAGE CHECK
FIRST CLASS
GATE
7
GATE CLOSES
19:30
SEAT
25 b
Class
First Class
Departure
New York
Arrival
Paris
R No
023 07654 00984
BOARDING PASS
FIRST CLASS
GATE:
7
GATE CLOSES:
19:30
SEAT
25 b

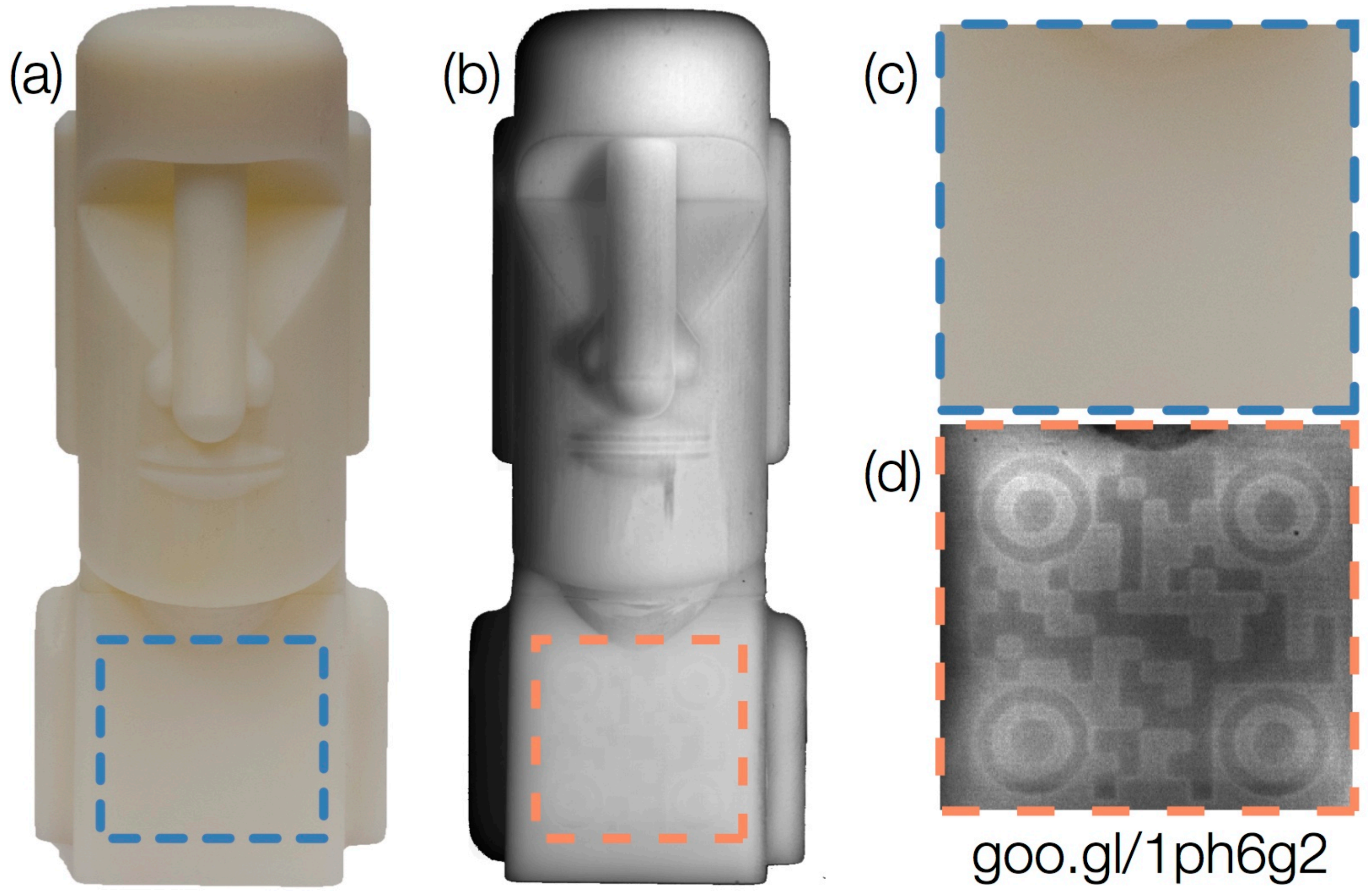

FAMILY SIZE
Lucky Charms
3 new Rainbows!
Gluten Free


THE NORTH FACE

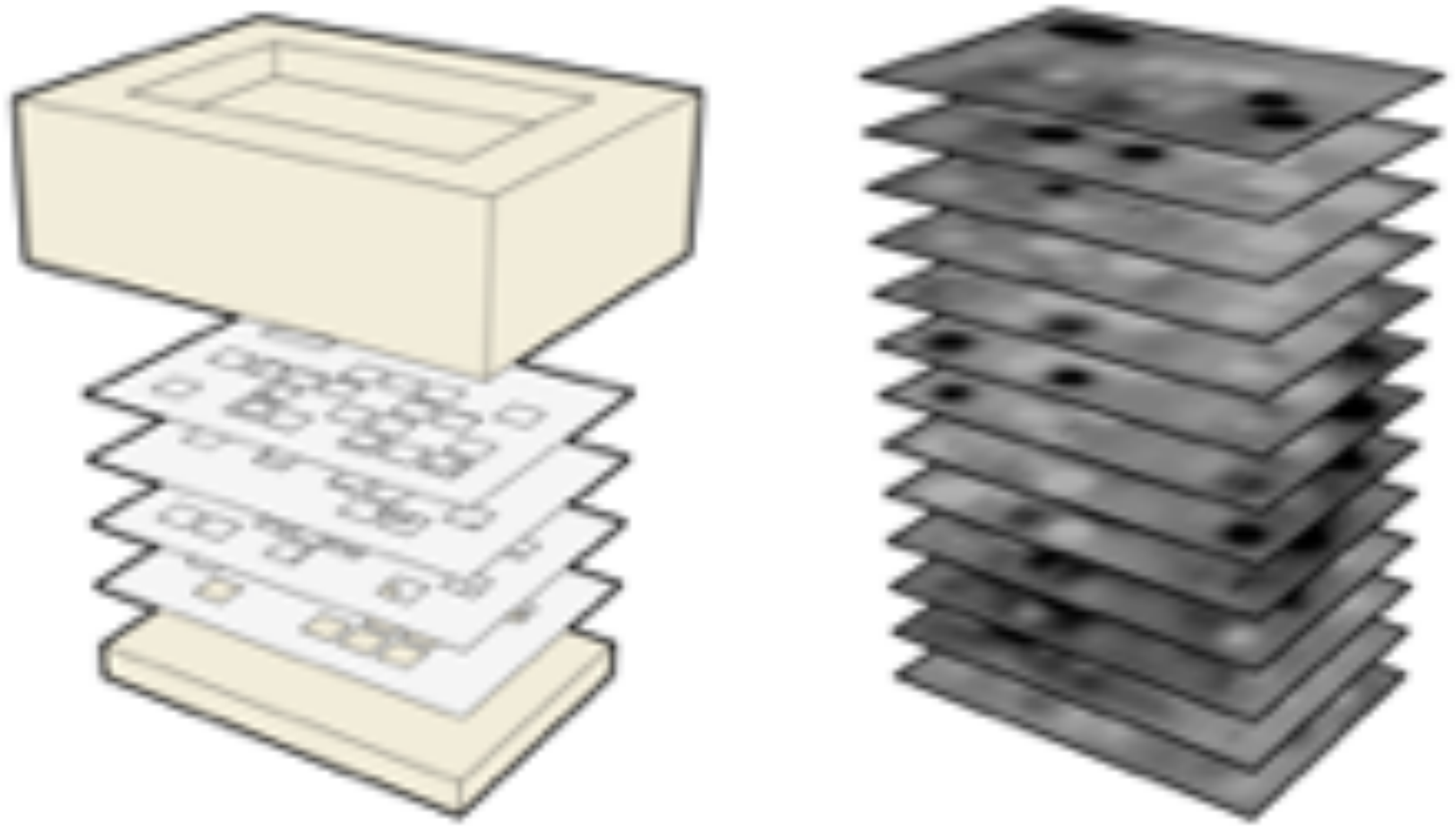
# 3D Encoding



surface



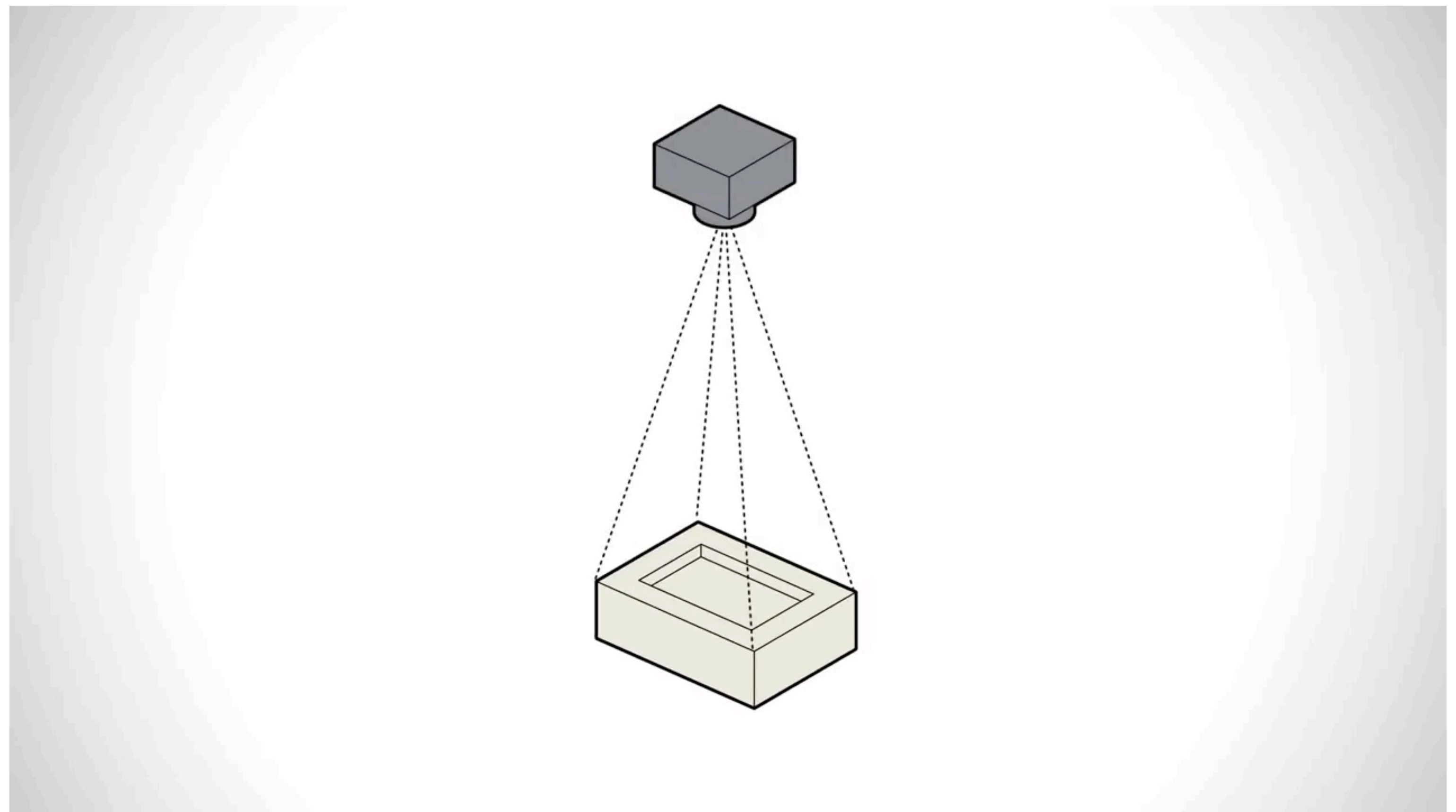

subsurface



internal

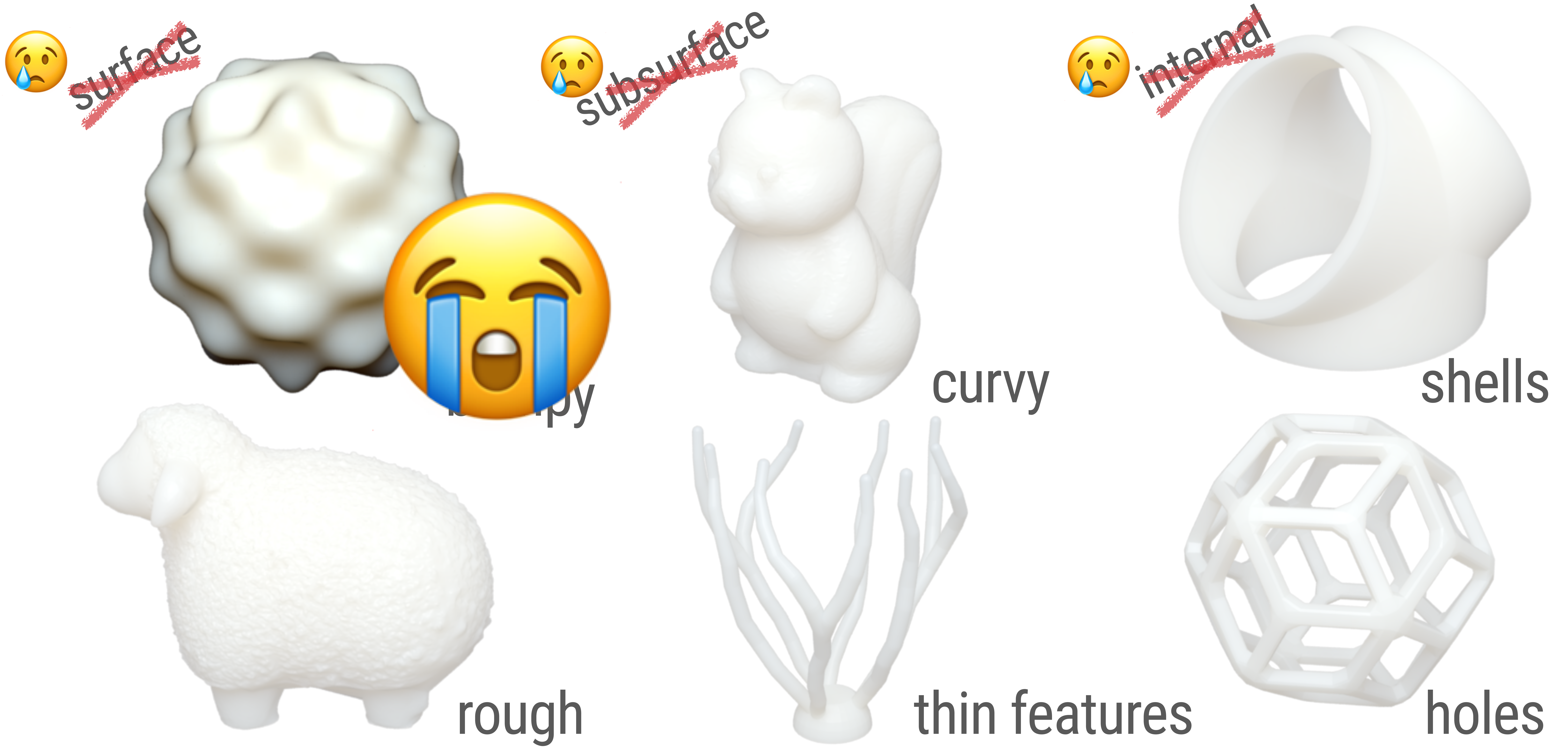
Acoustic Barcodes
[Harrison et al. 2012]


AirCode
[Li et al. 2017]

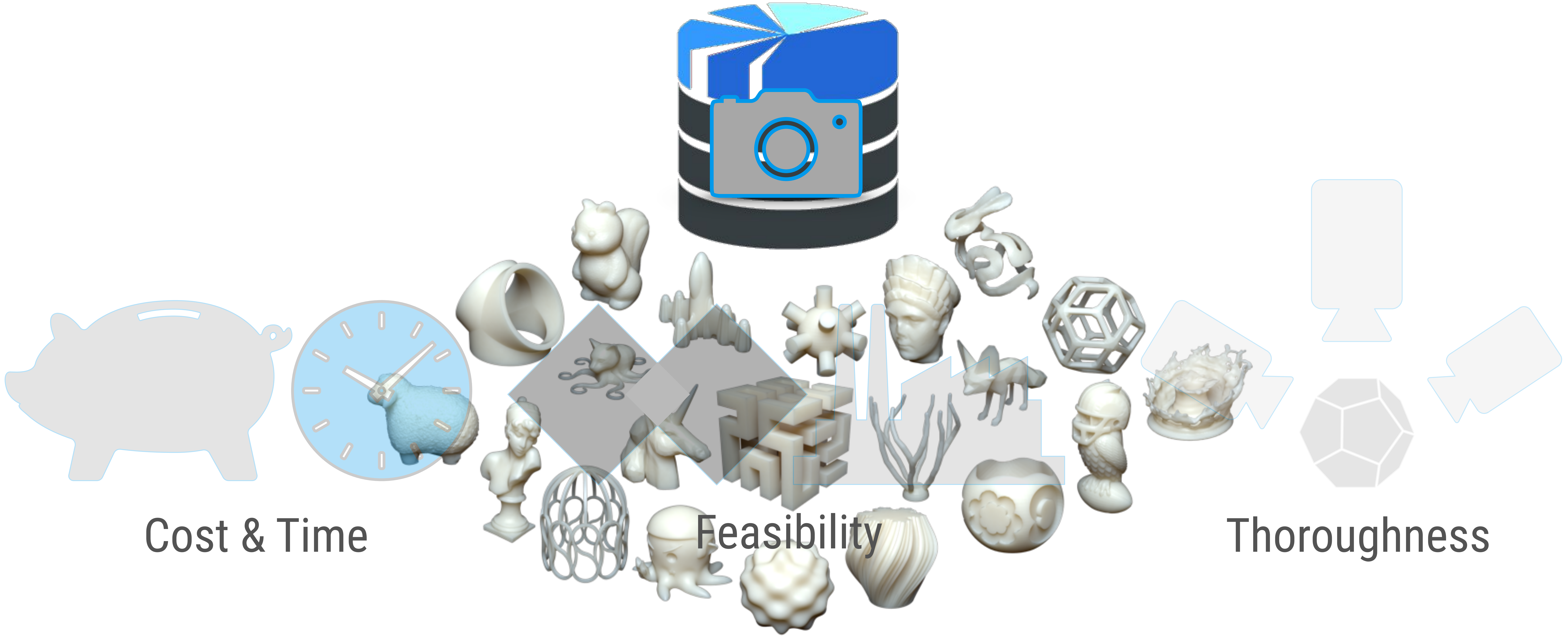


Infrastructures
[Willis and Wilson 2013]

# 3D Shapes: Hard to Tag



# Synthetic Shape Exploration




Decode
take a photo
10101001


Ultimaker 2
Extended
layer by layer

# Layer by Layer Fabrication

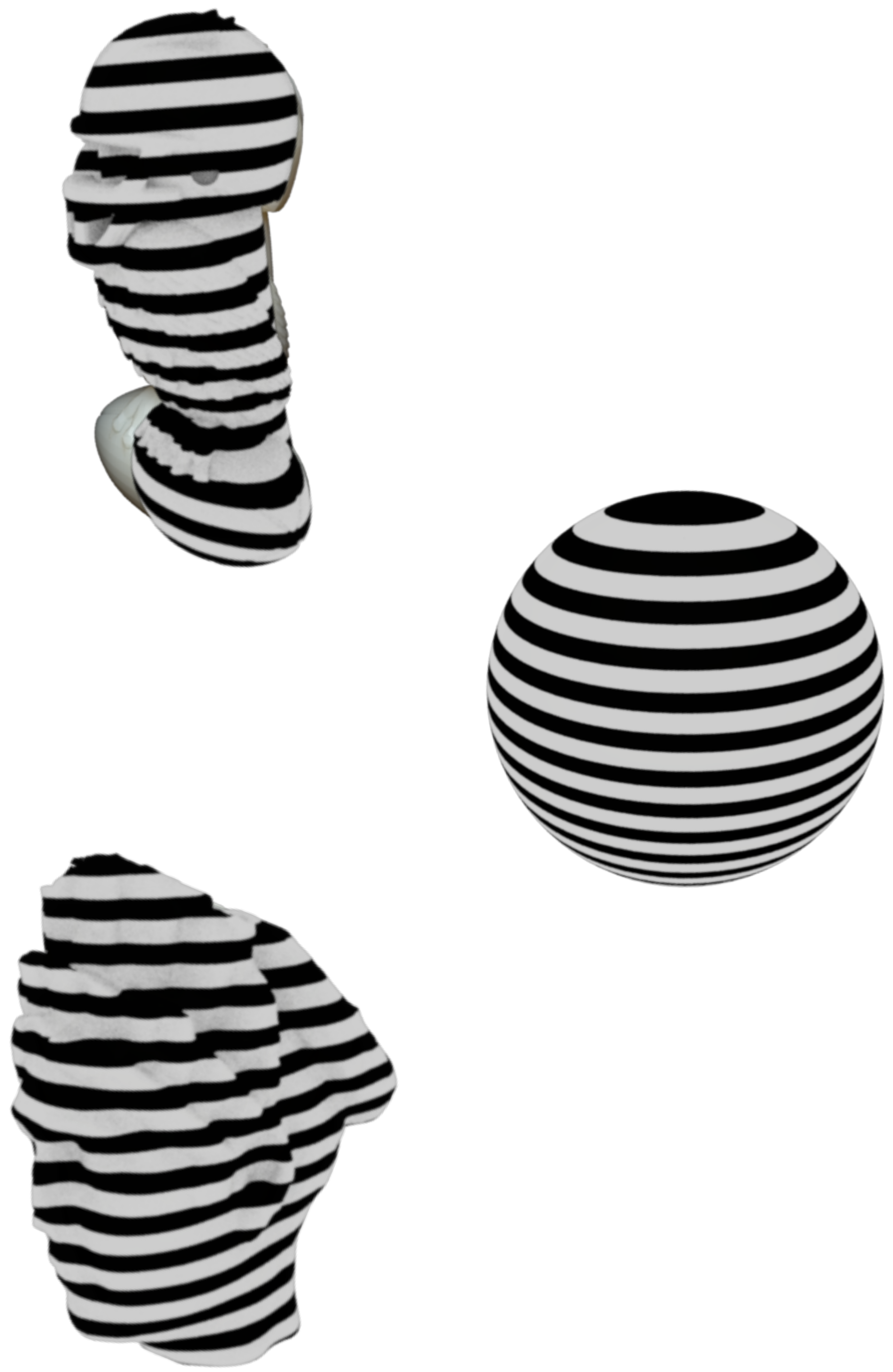
**Key Idea**

Additive Manufacturing

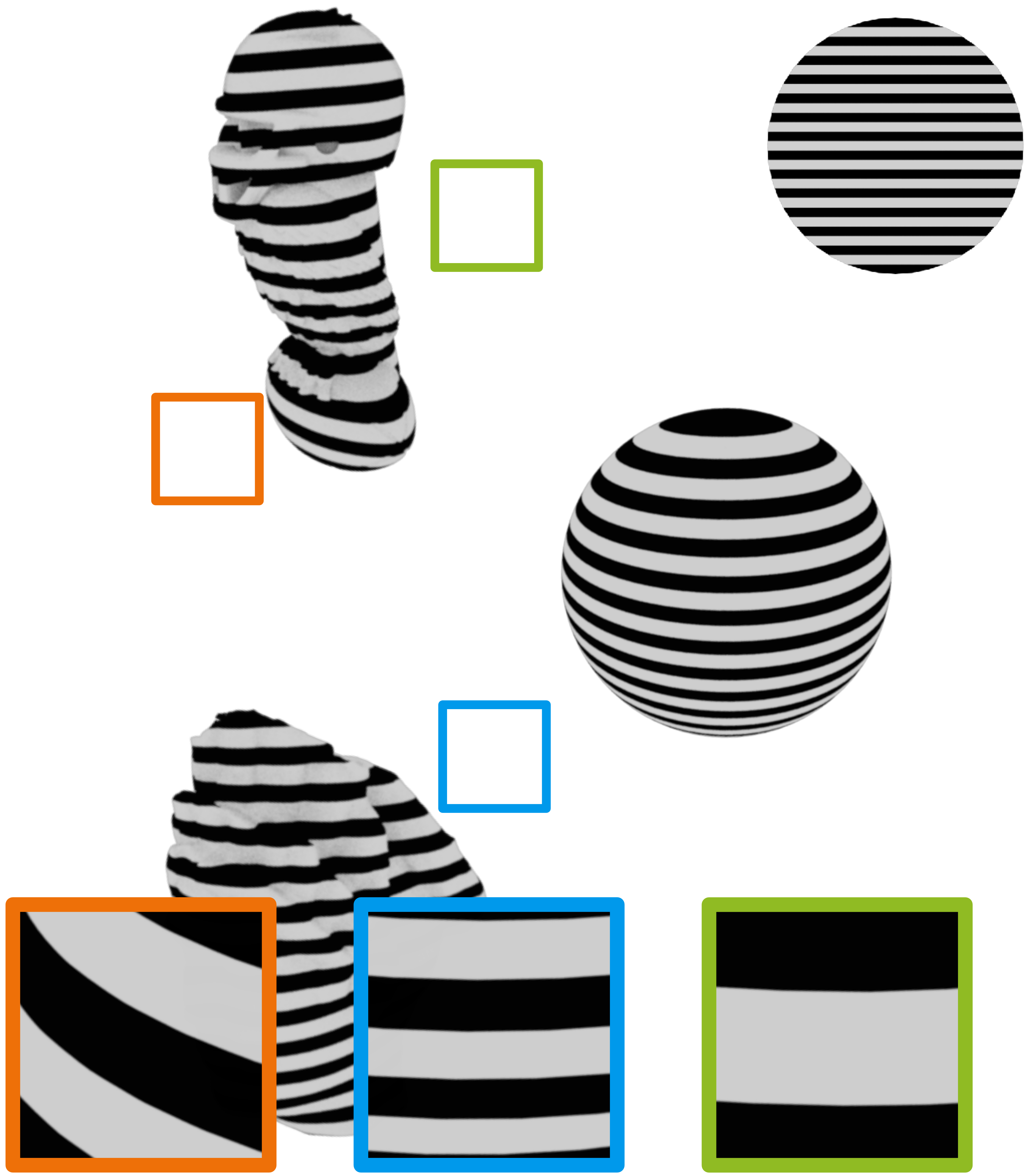
LayerCode

e.g. 3D Printing

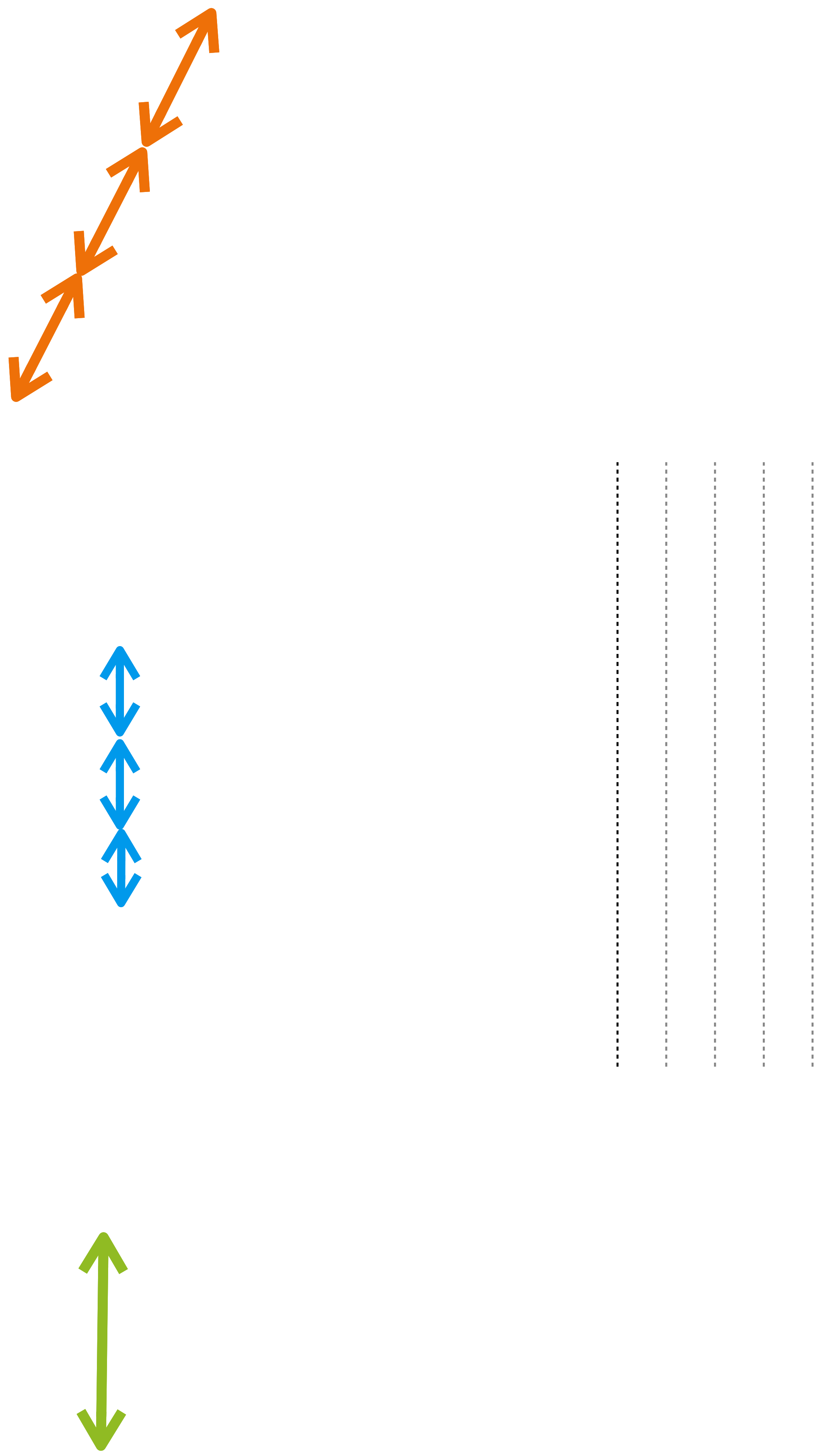
# Encoding Global Lengths

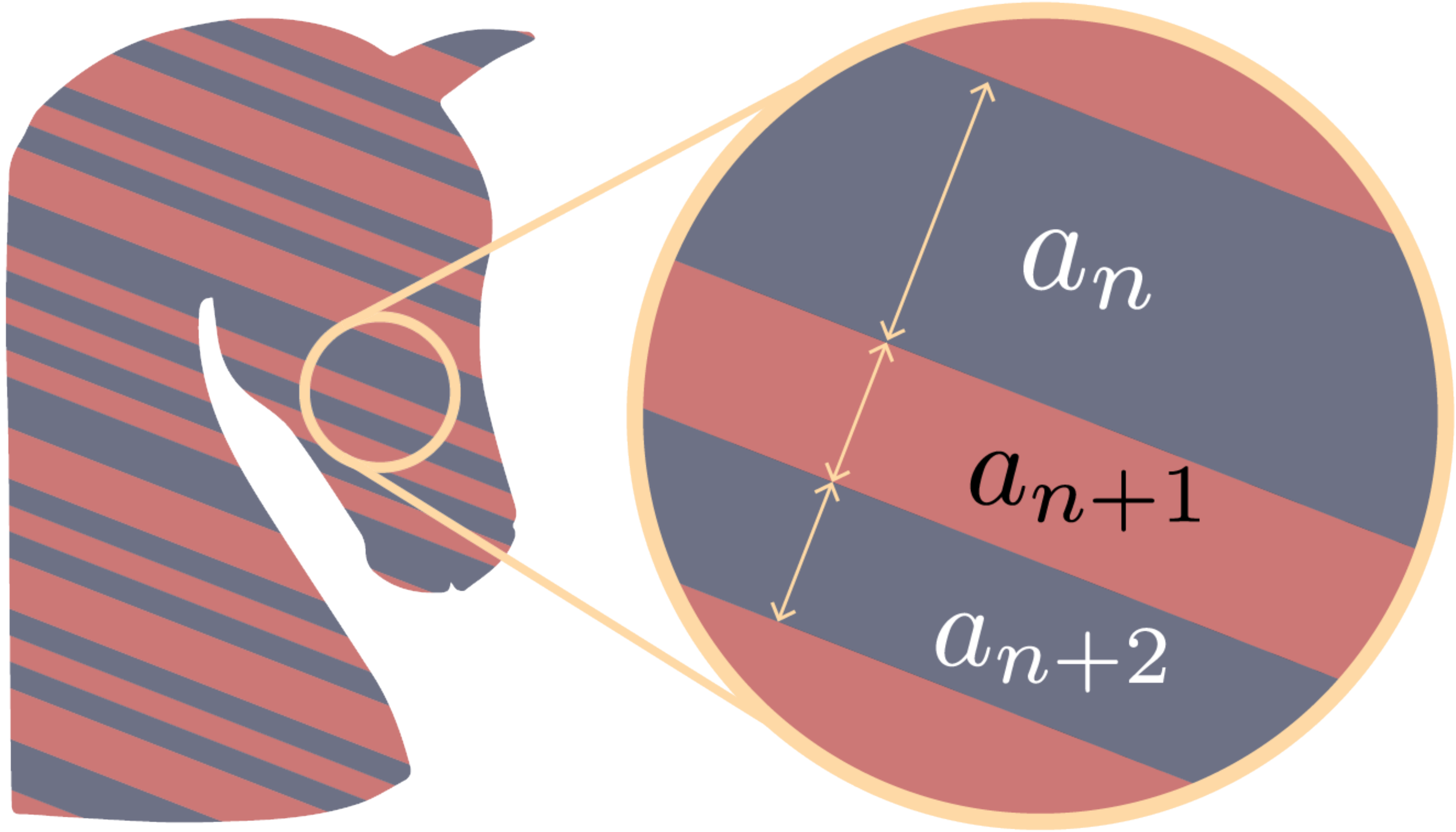



# Encoding Global Lengths

# Encoding Local Ratios

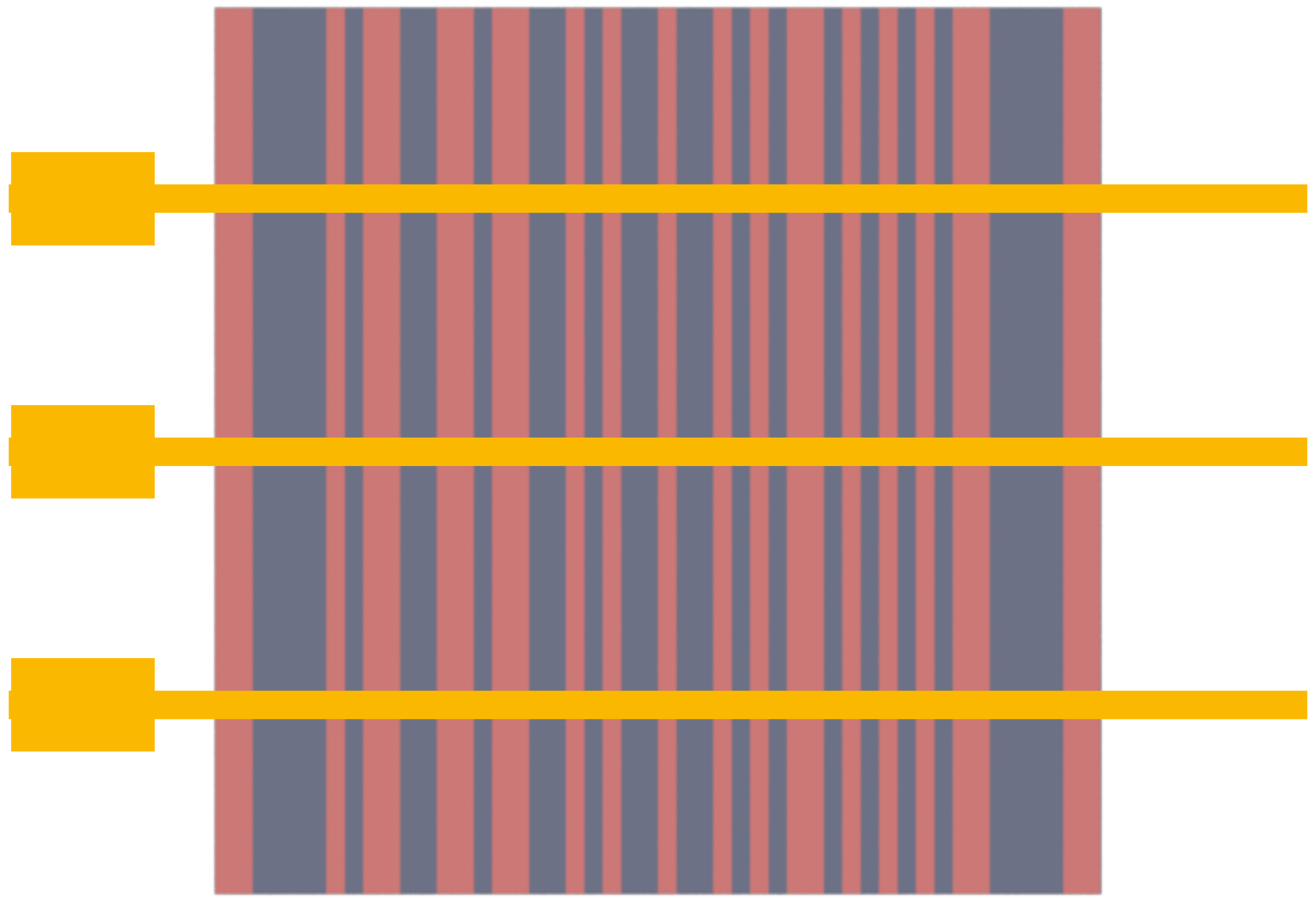




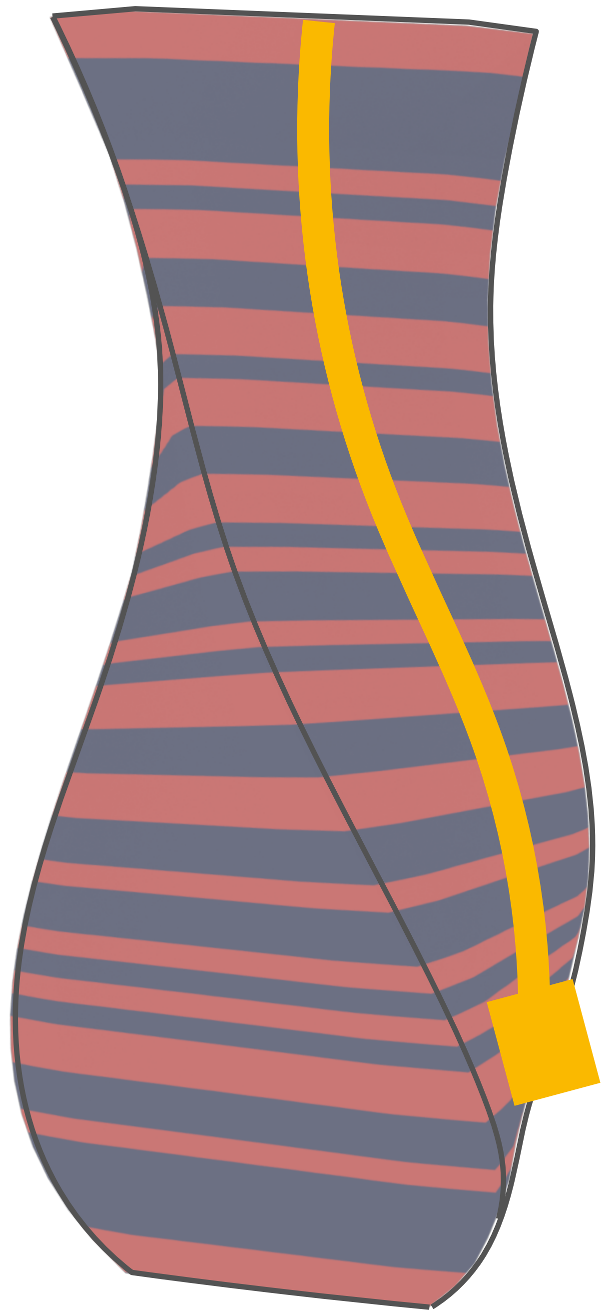


Binary LayerCode Encoding

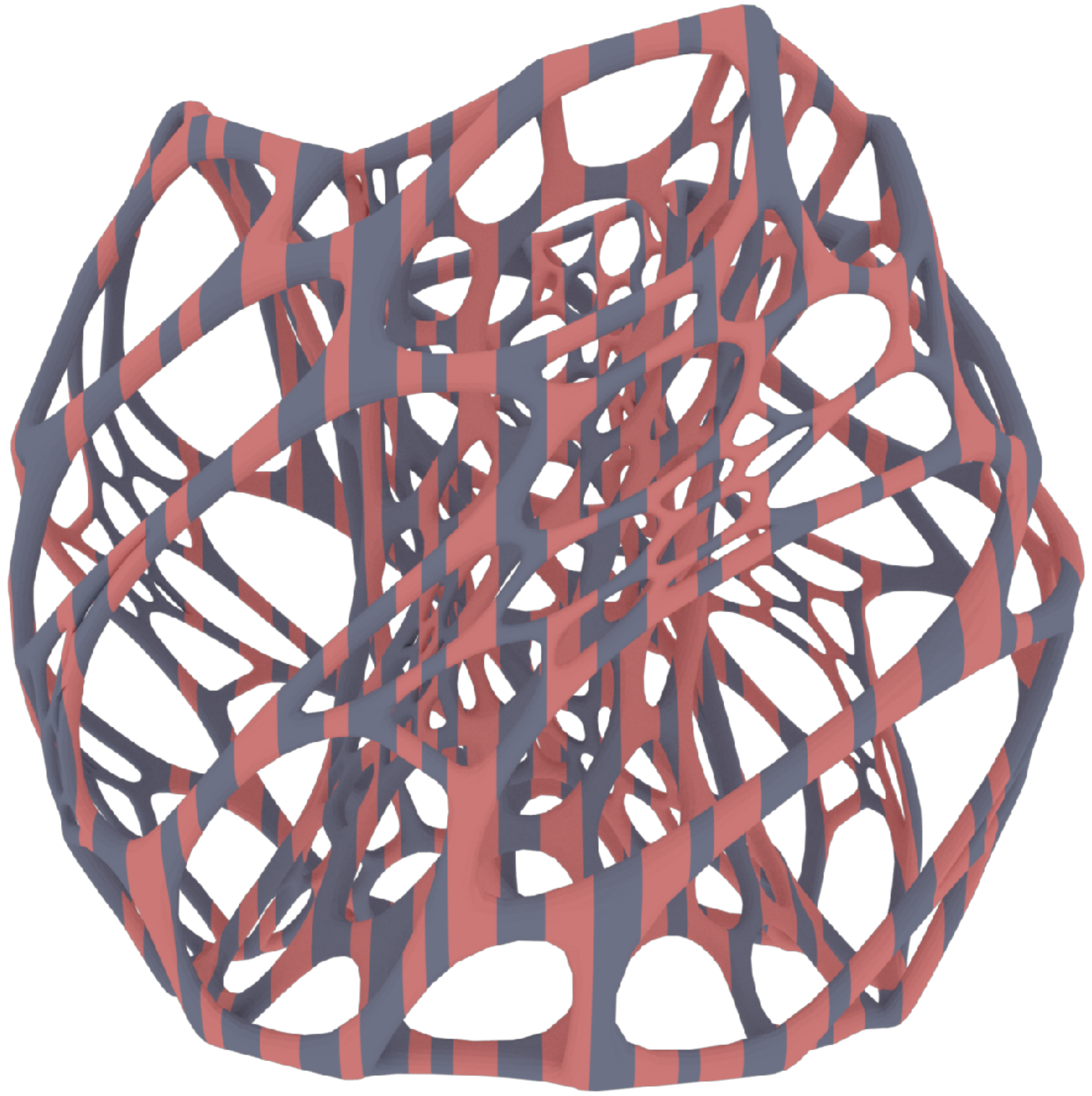
# Decoding



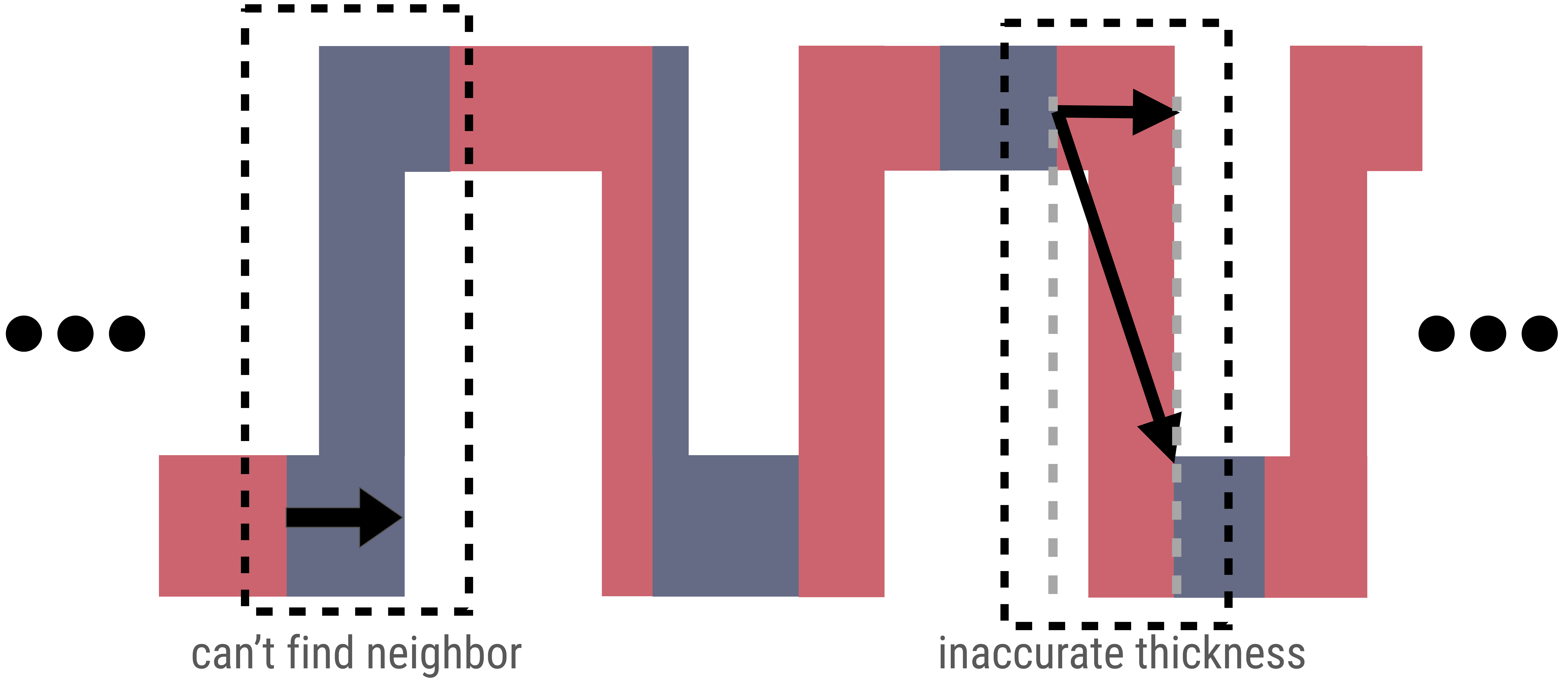
multi-linear scan



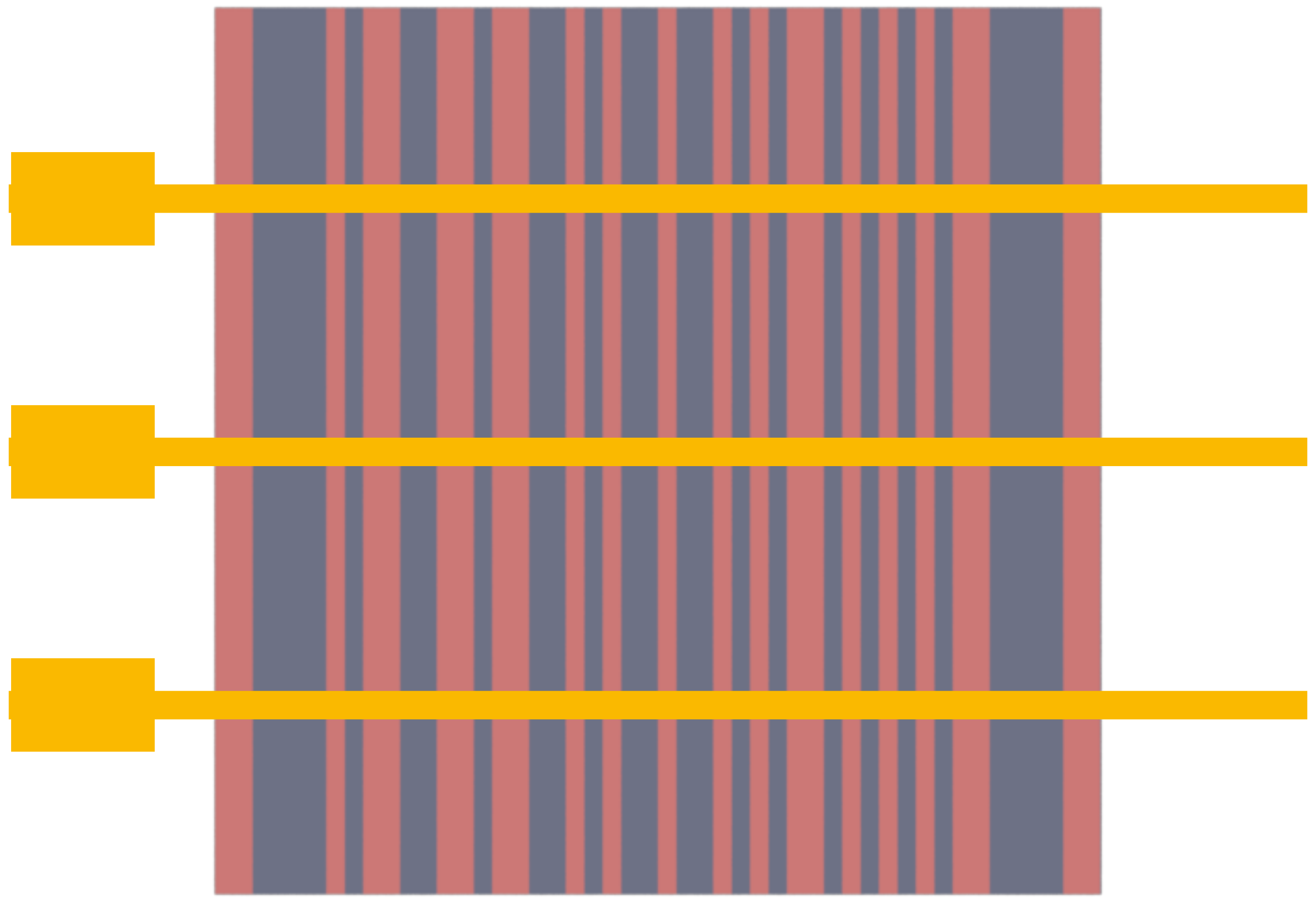
non-linear scan



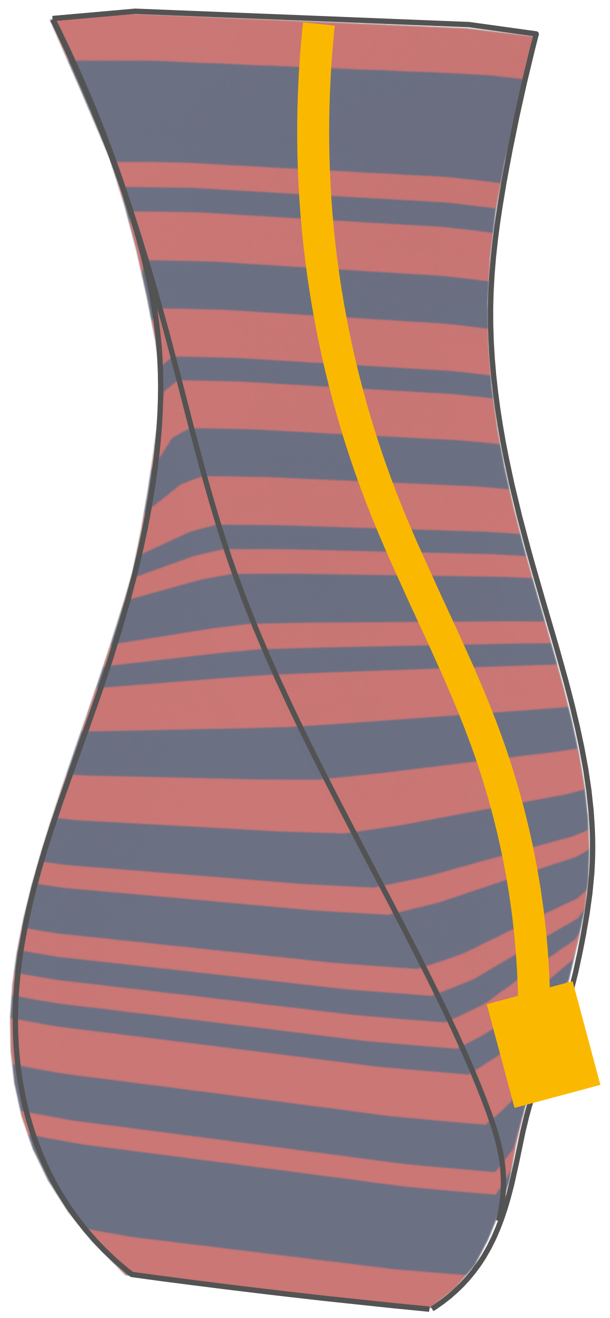
# Computing Robust Ratios



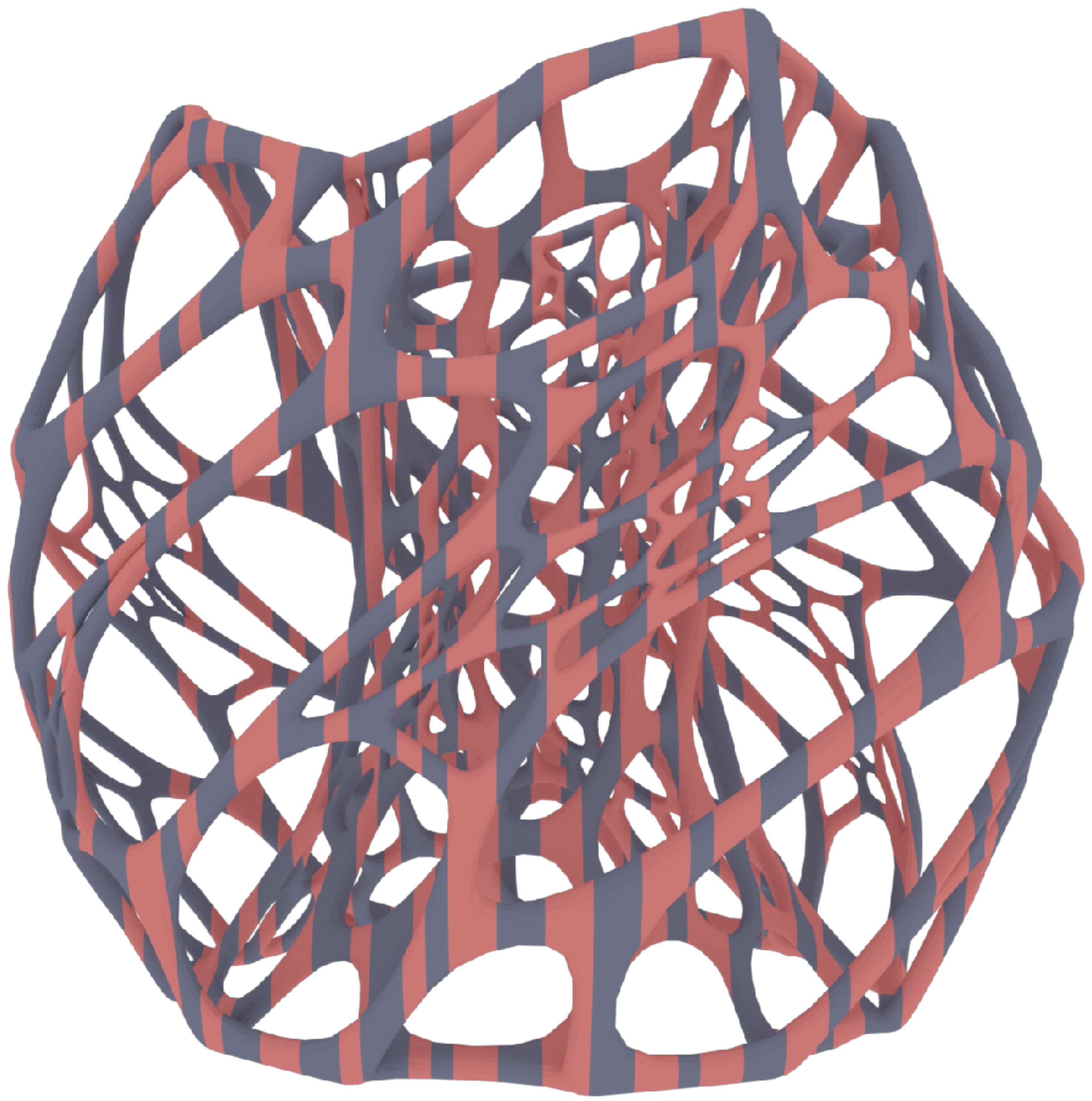
# Decoding



multi-linear scan

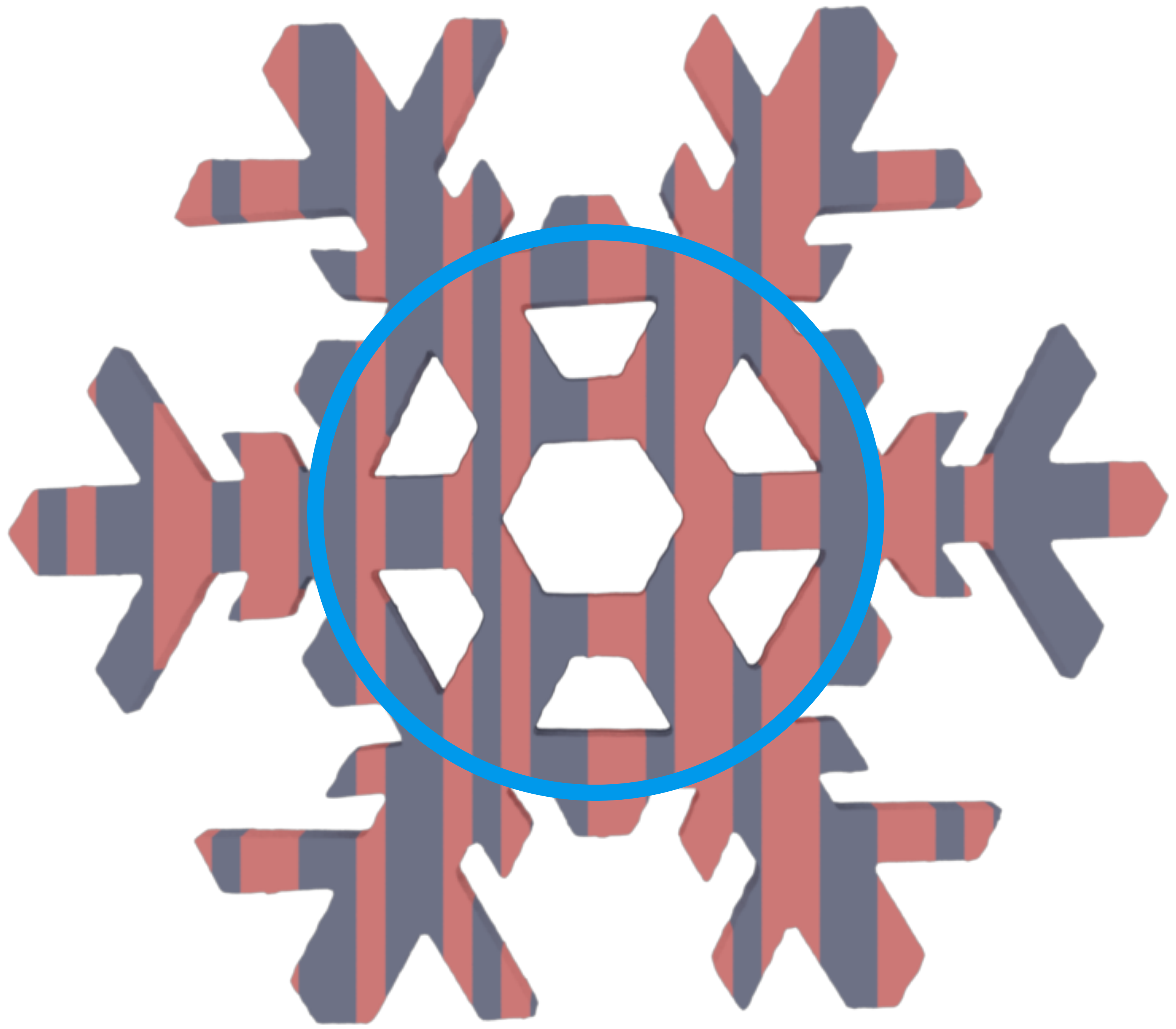


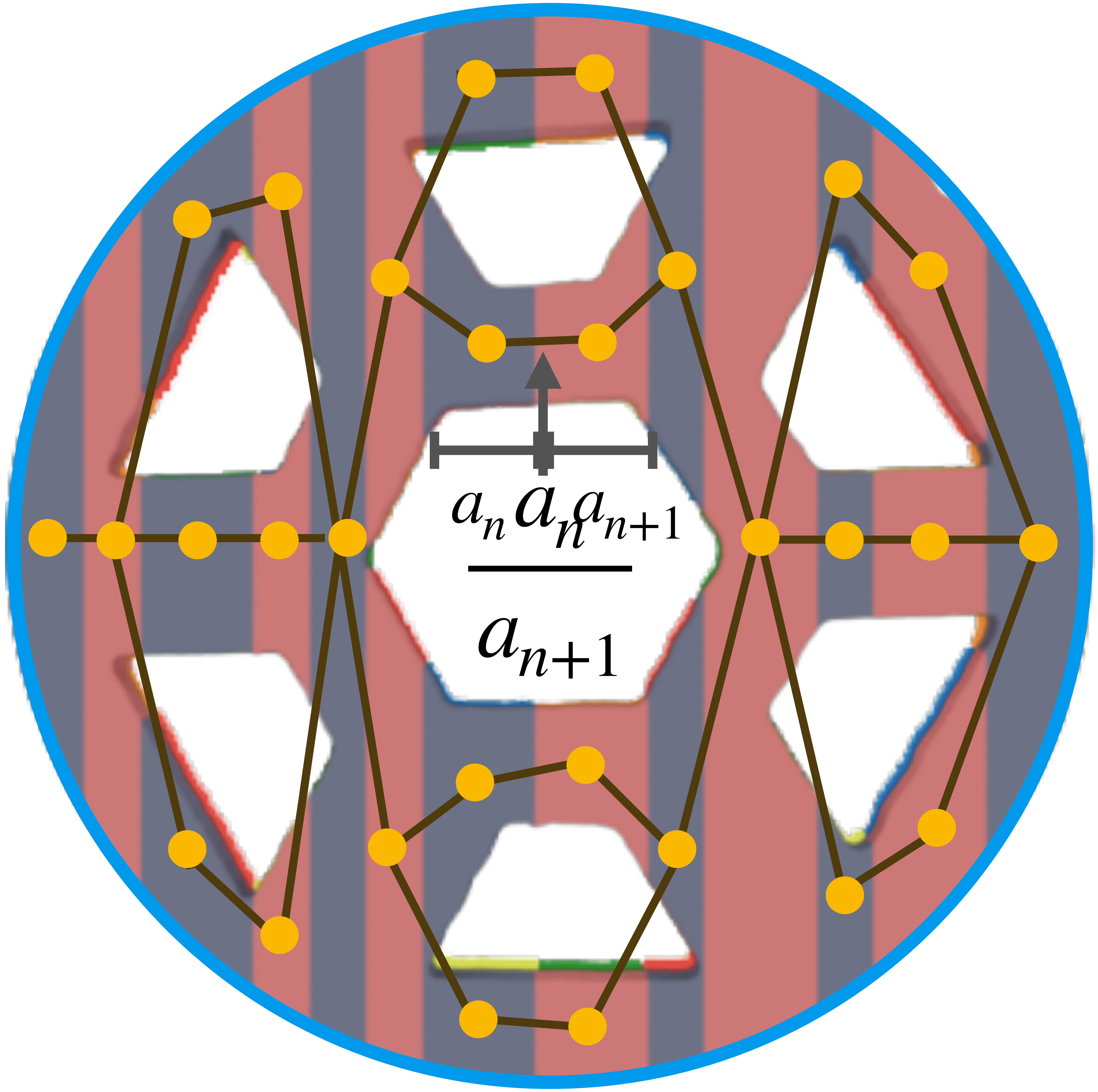
non-linear scan



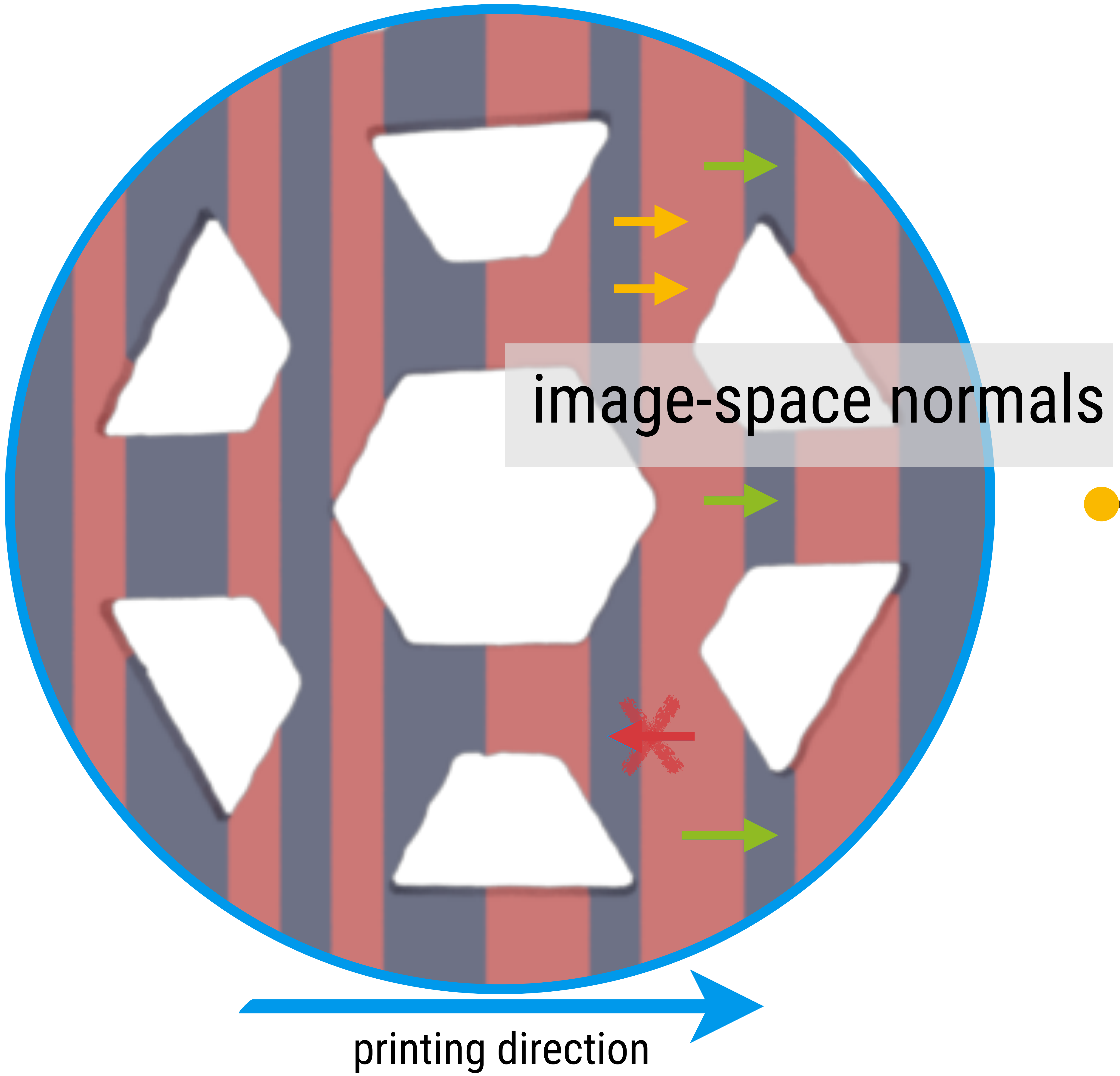
graph-based approach

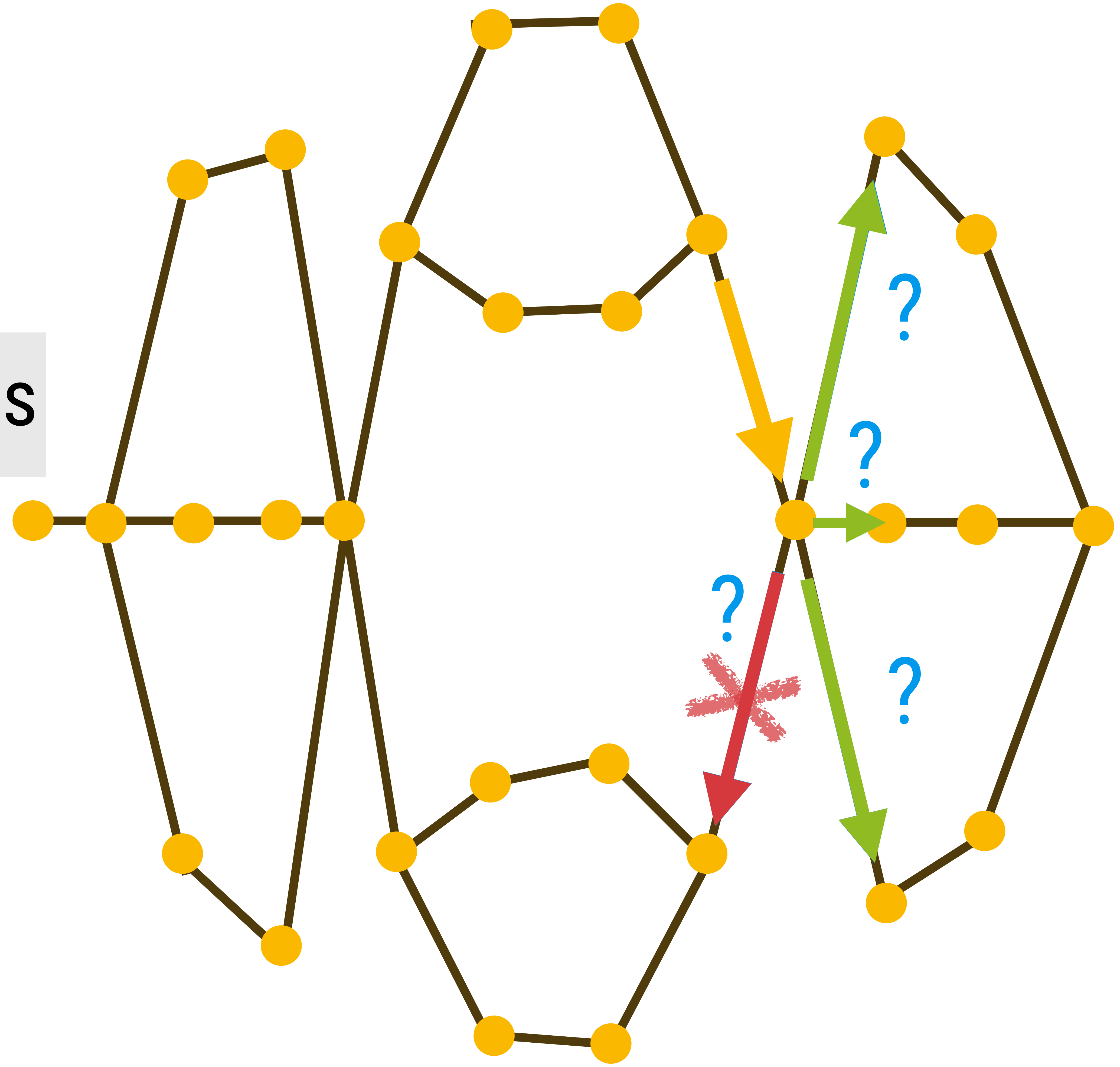
# Decoding: graph extraction



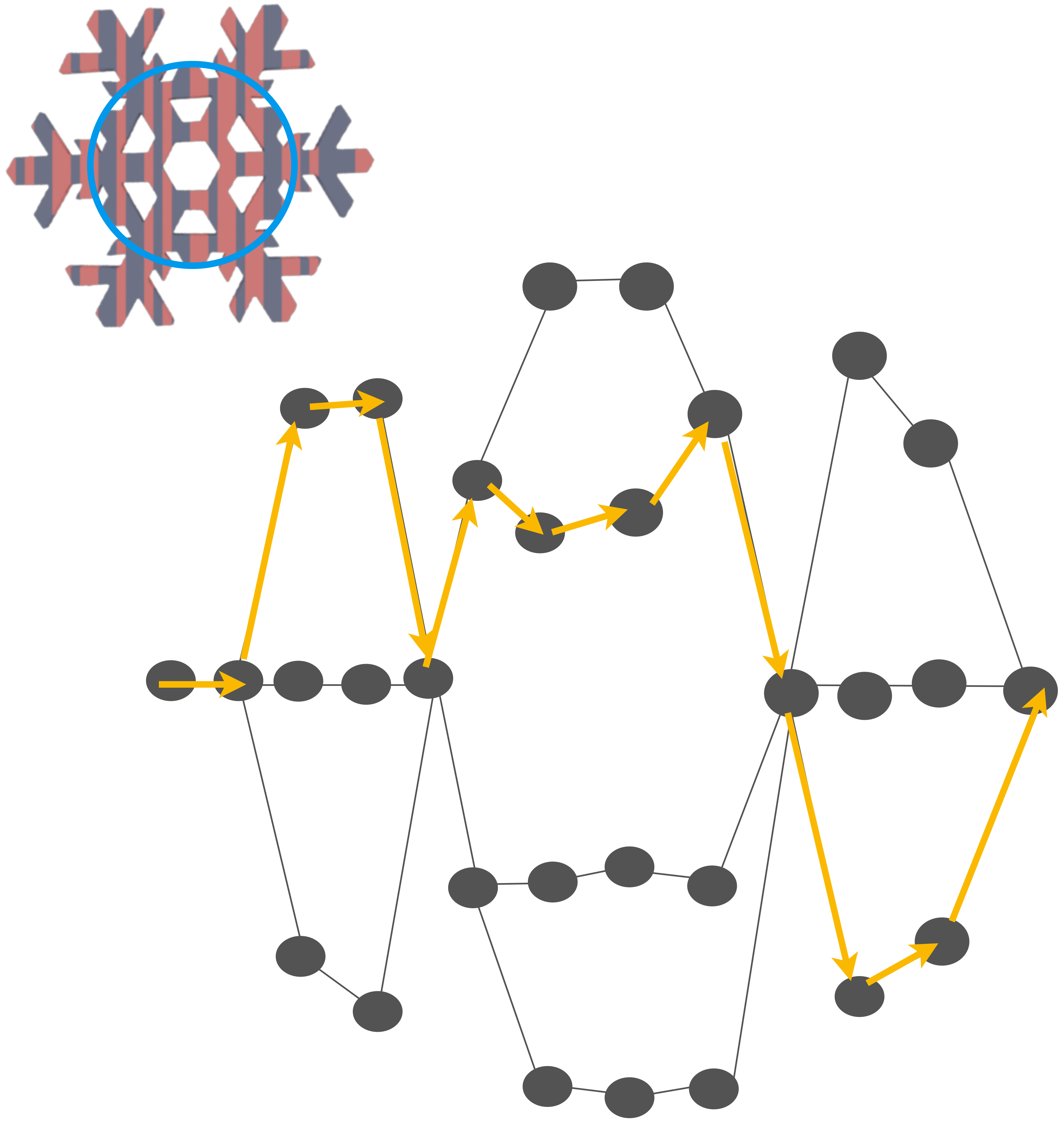


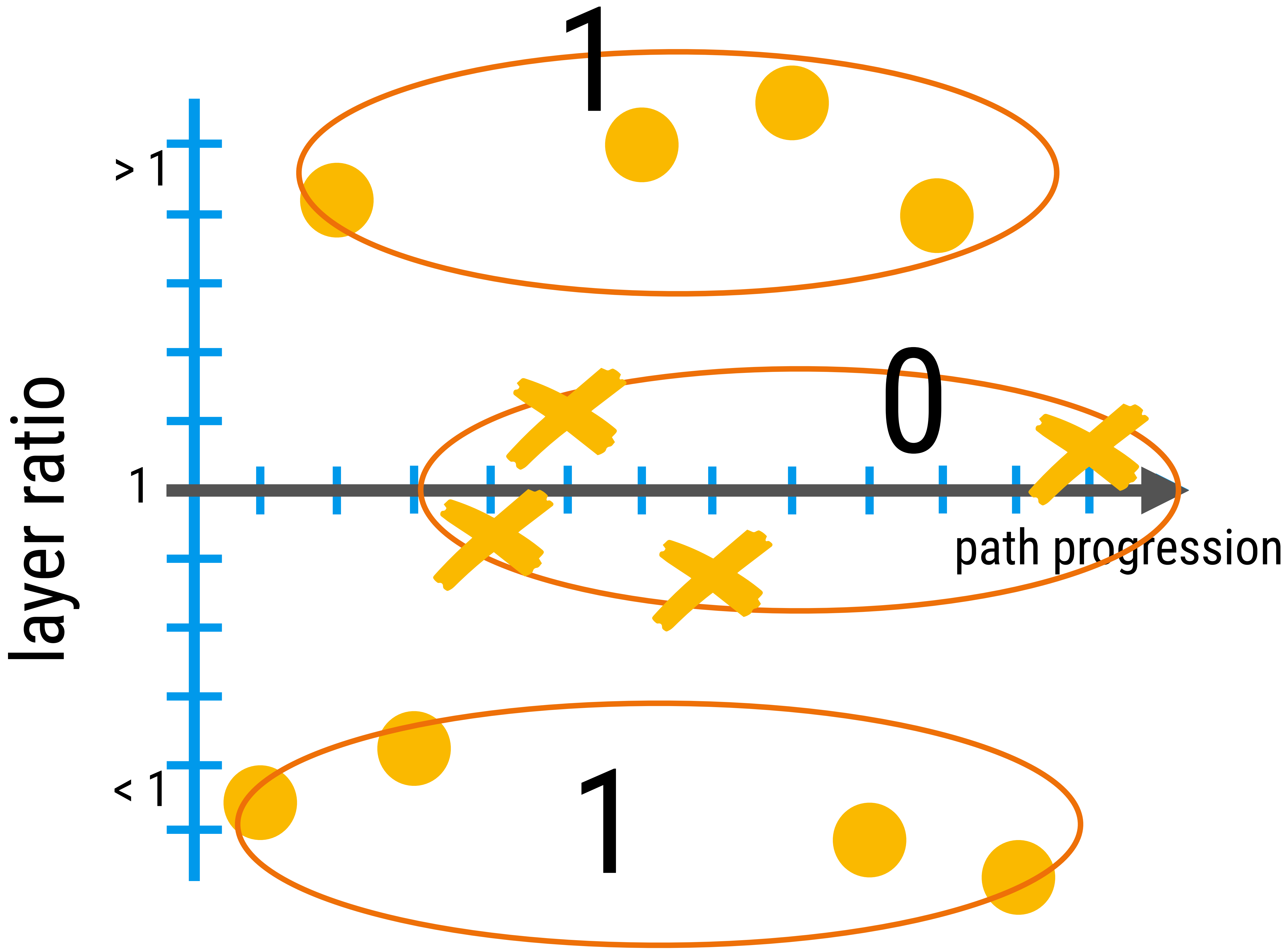
# Decoding: graph extraction cont.



# Decoding

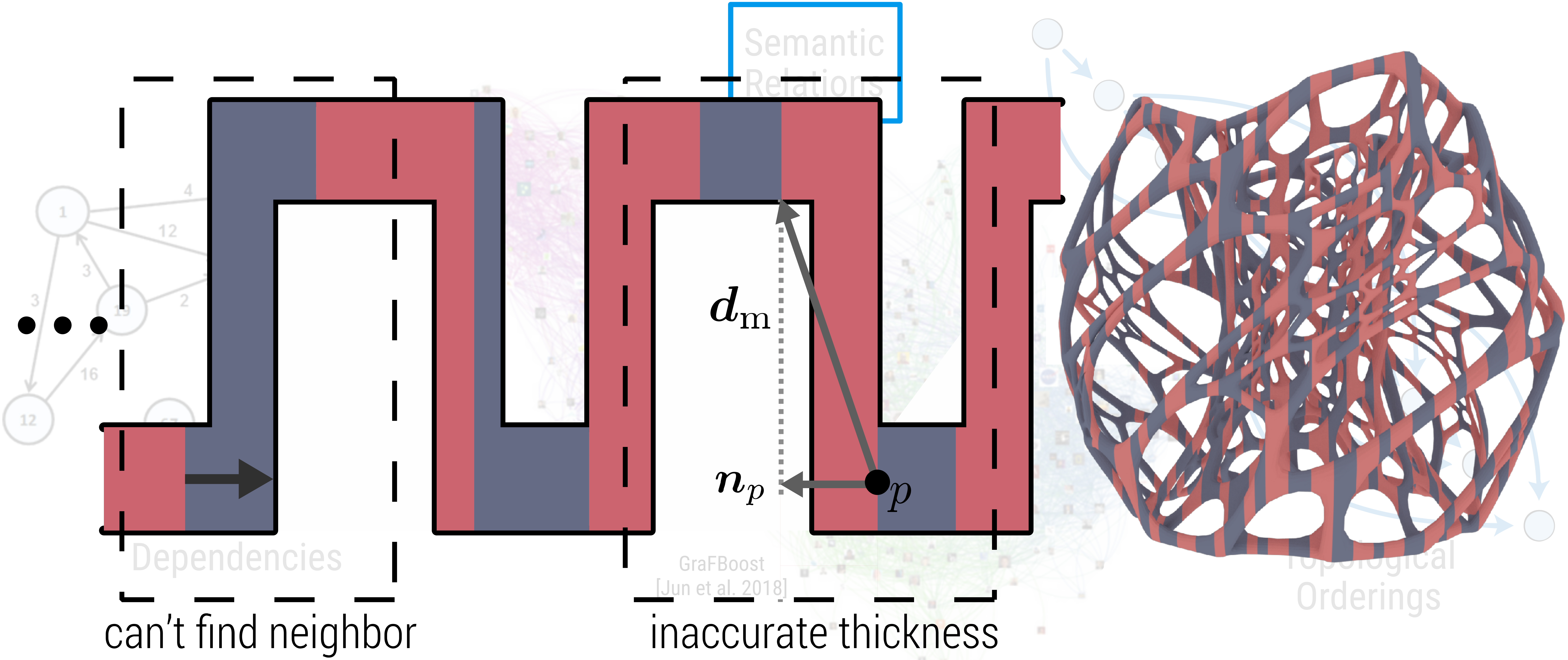





$$a_n \not\approx a_{n+1} \Rightarrow 1, \quad a_{n+1} \approx a_{n+2} \Rightarrow 0$$

code: 111001011110

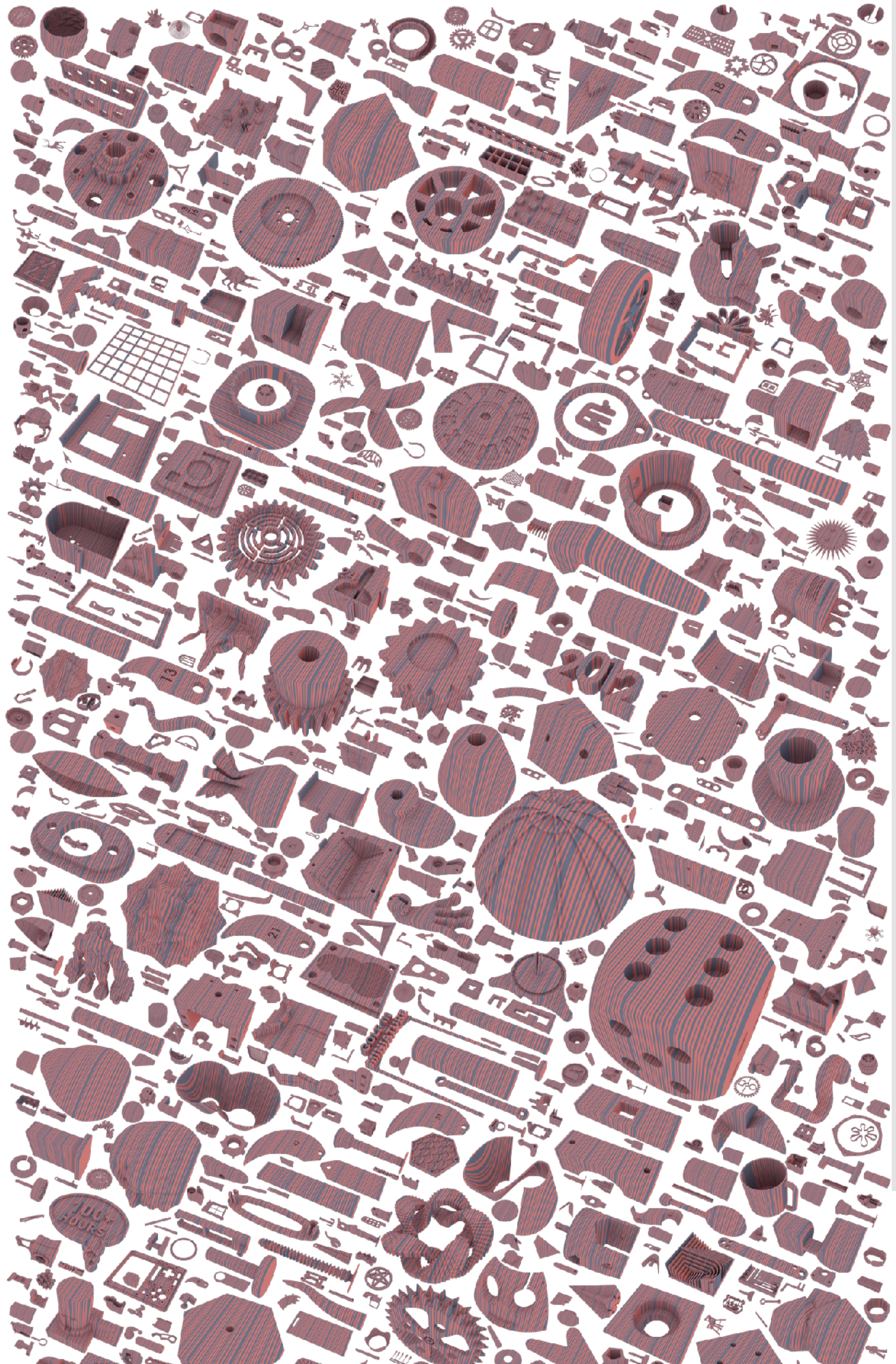
# LayerCode Graphs



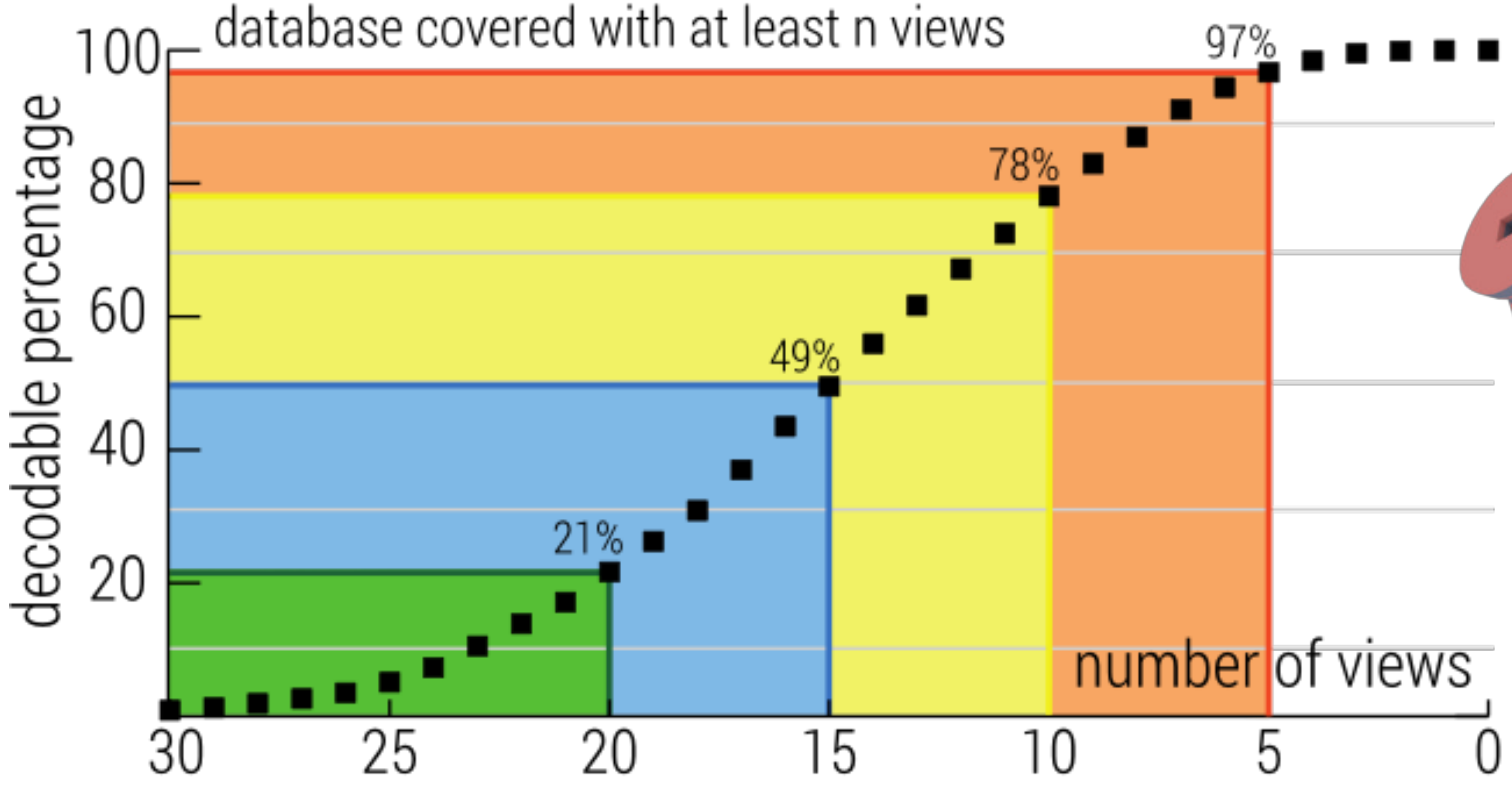
# Virtual Evaluation on Thingi10K

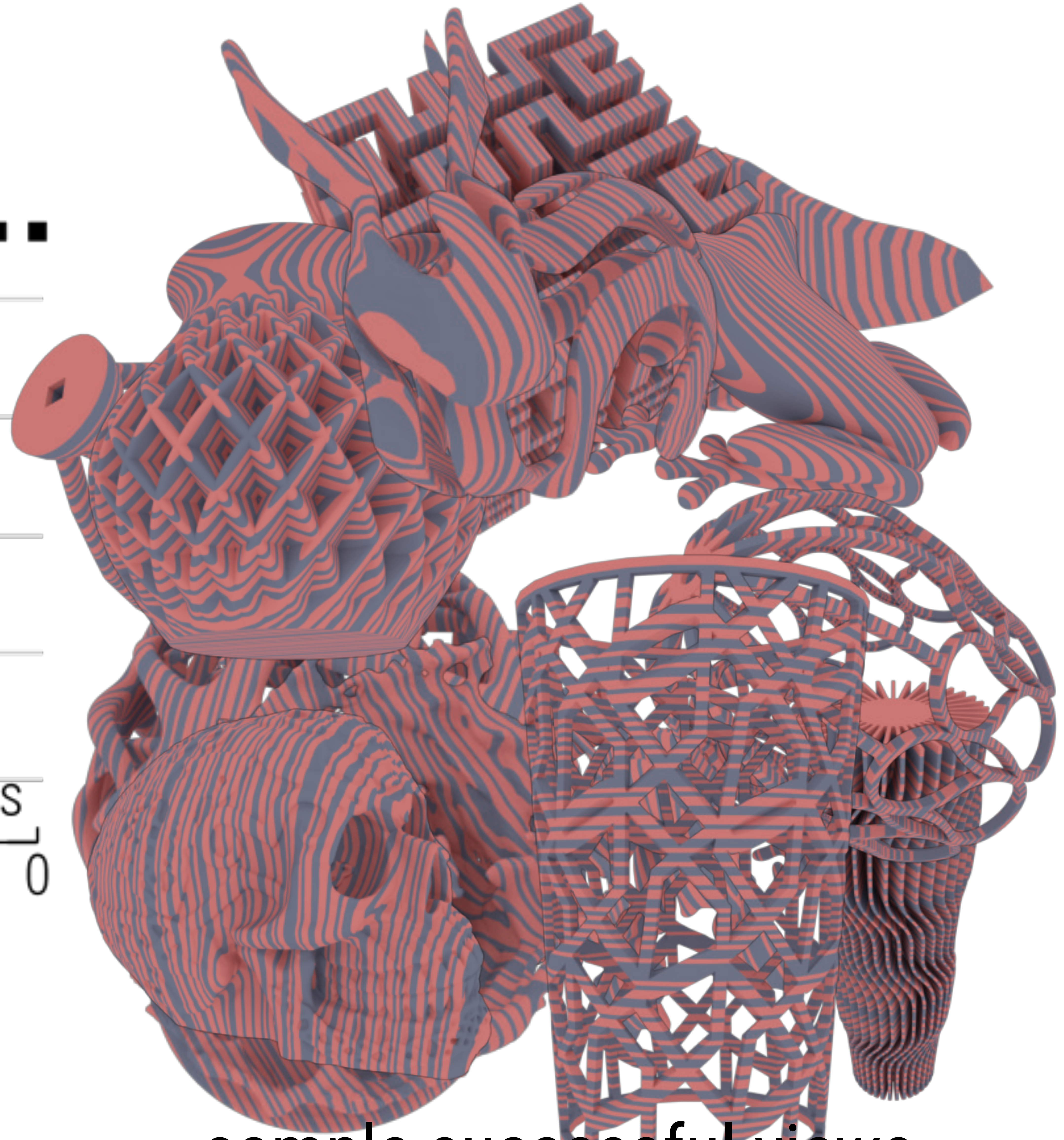
**4,835 meshes**

**145,050 images**



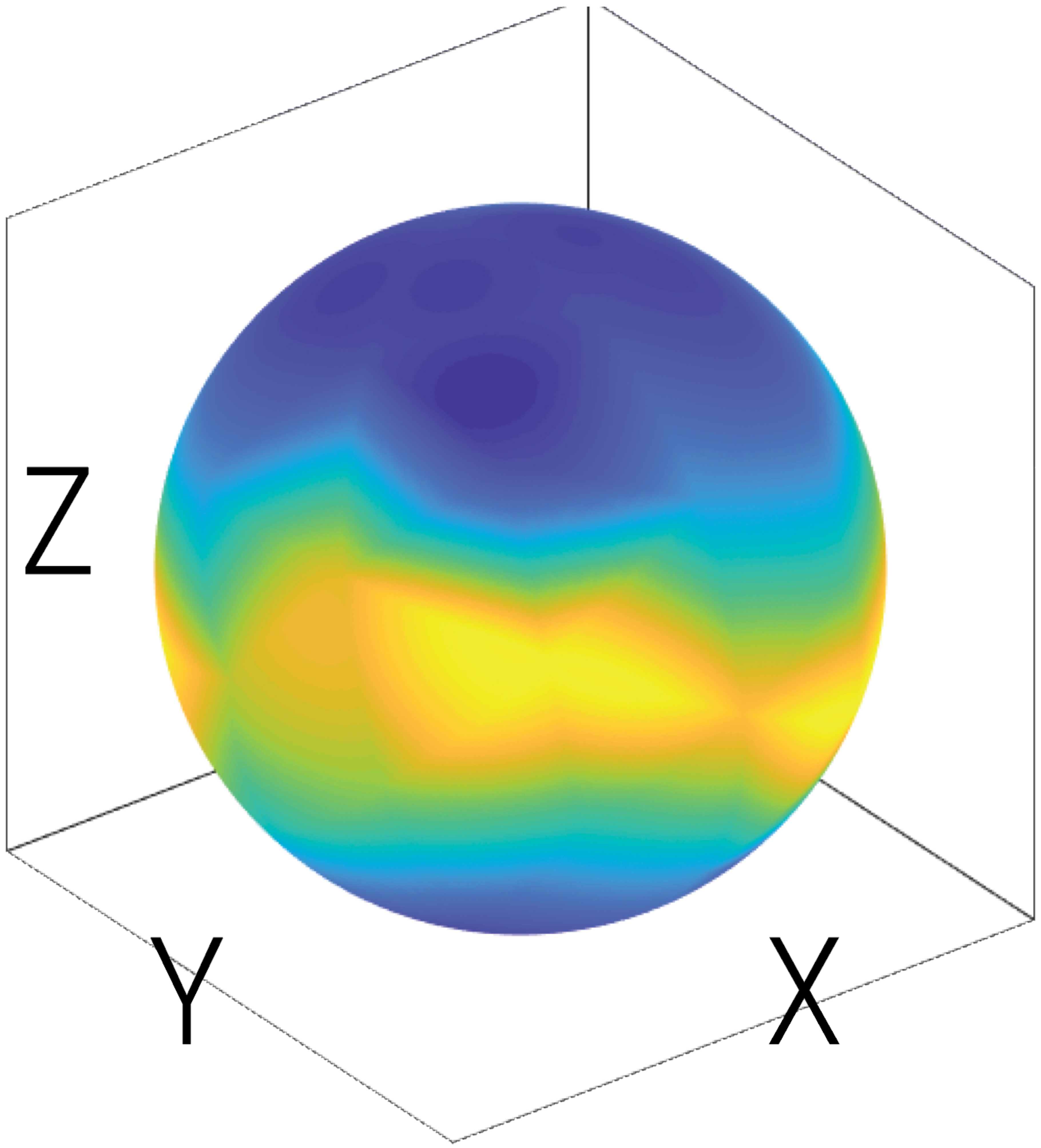
# Virtual Evaluation of Decoding Database

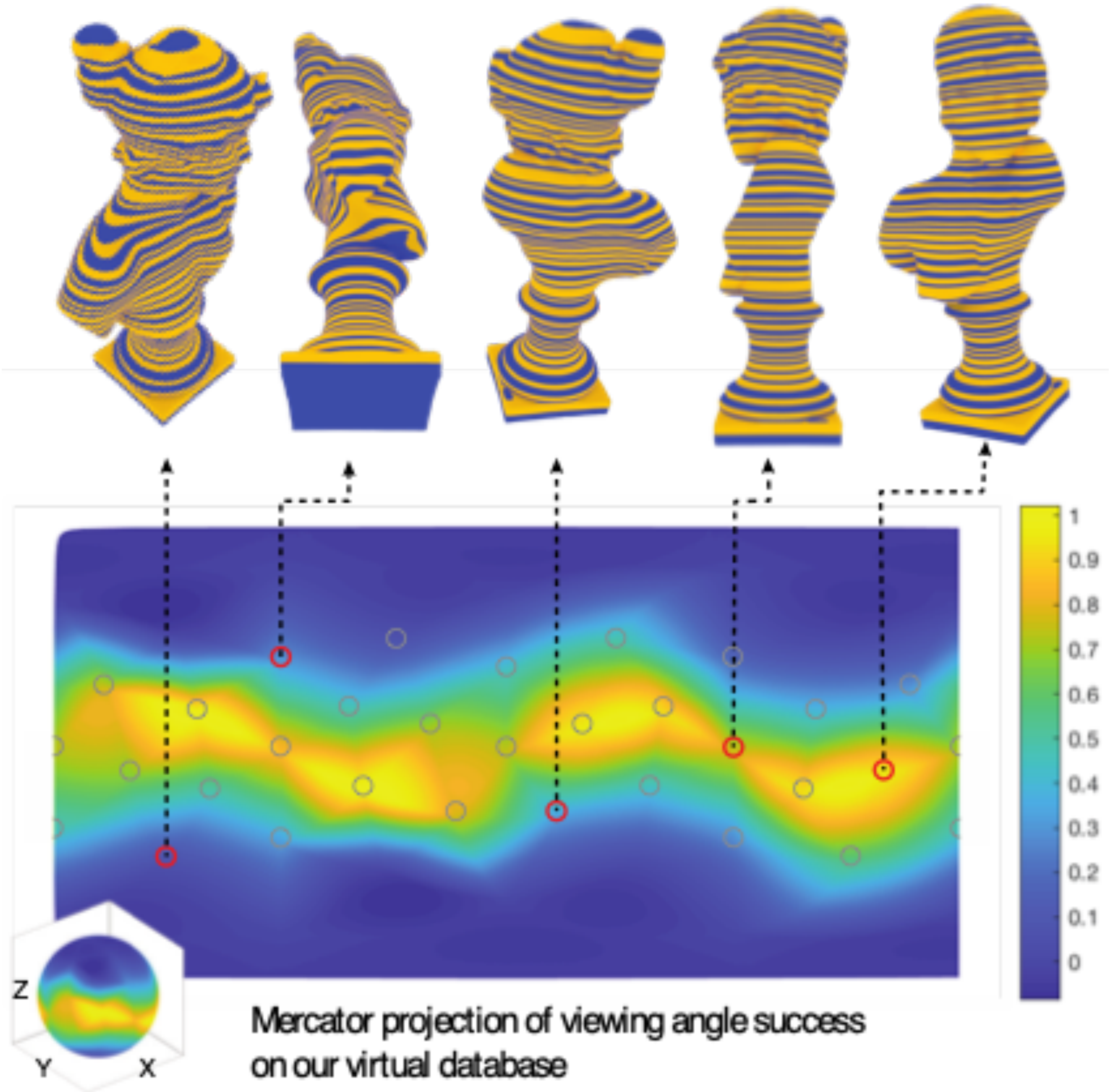


sample successful views

# Virtual Evaluation of Views




Mercator projection of viewing angle success on our virtual database

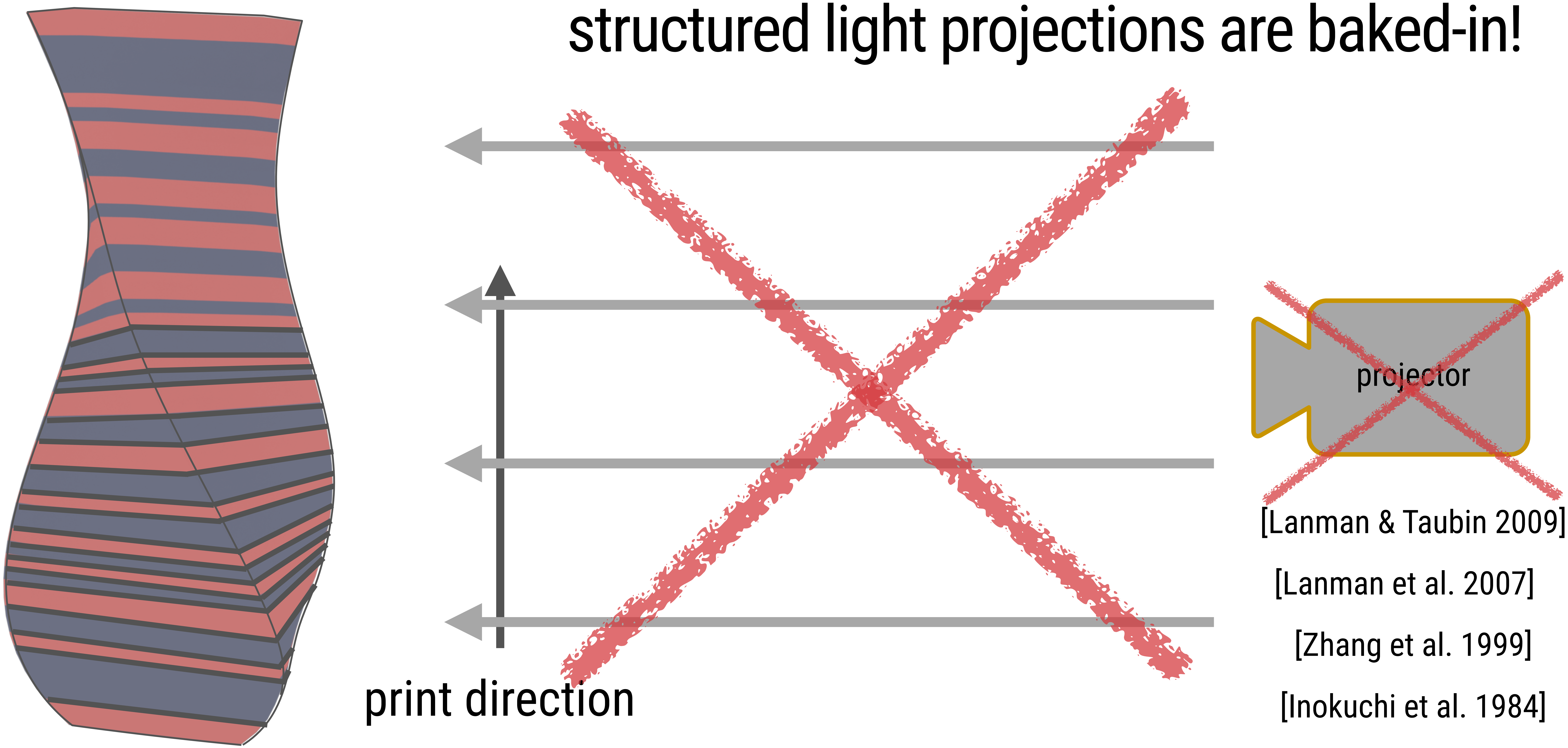
# Physical Hyperlinks

Sample Query Information:

```
#Vertices      : 2450
Euler          : 2
Genus          : 1
Closed         : True
Solid          : False
Edge manifold      : True
Duplicated faces : False
```

can we extract more than just the bits?

# What about 3D info?




[Lanman & Taubin 2009]

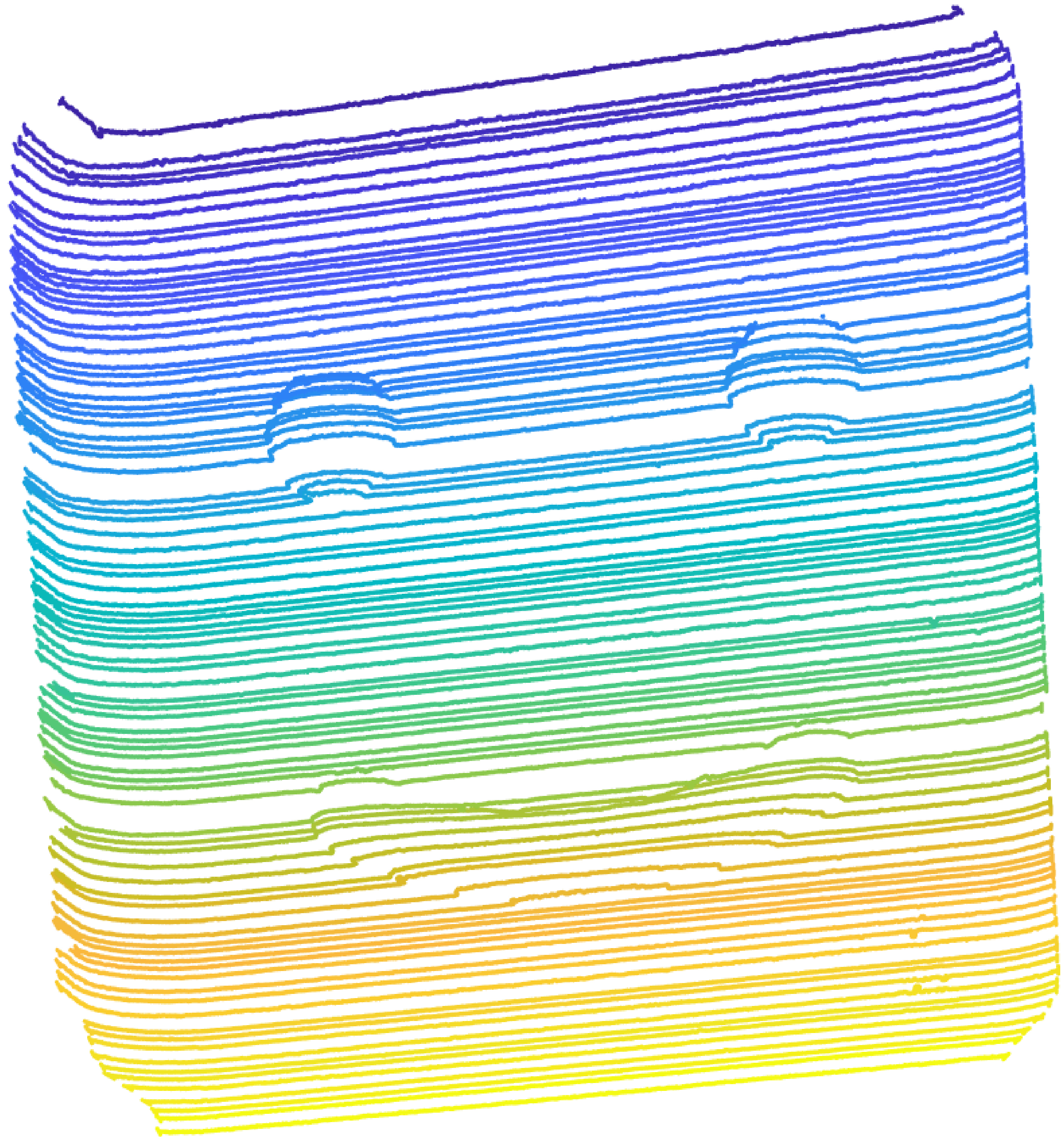
[Lanman et al. 2007]

[Zhang et al. 1999]

[Inokuchi et al. 1984]

# Free Depth Information


single image input

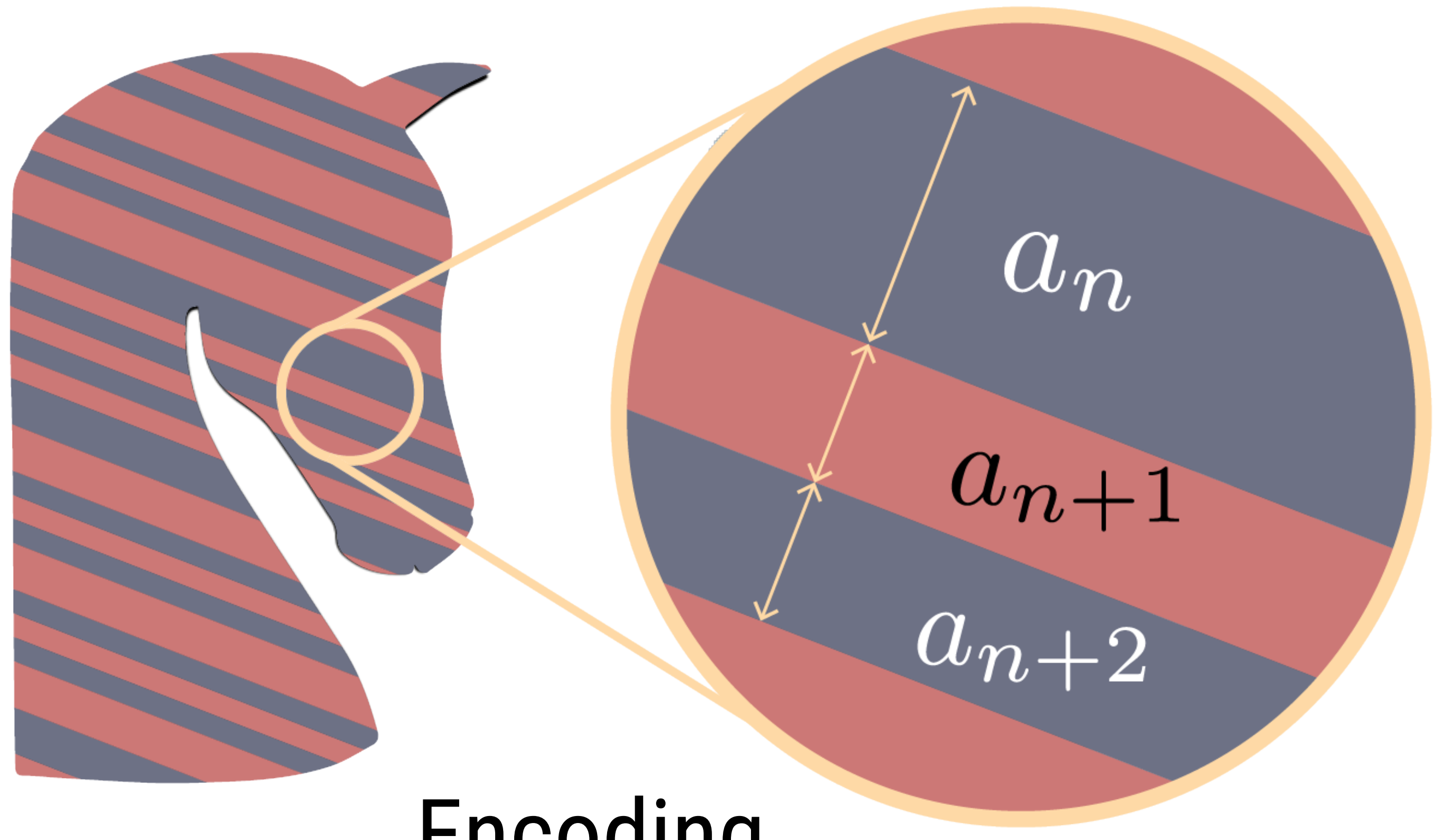

recovered 3D layers

# Ubiquitous tagging

LayerCode tags objects on the inside as well


Virtual Repair

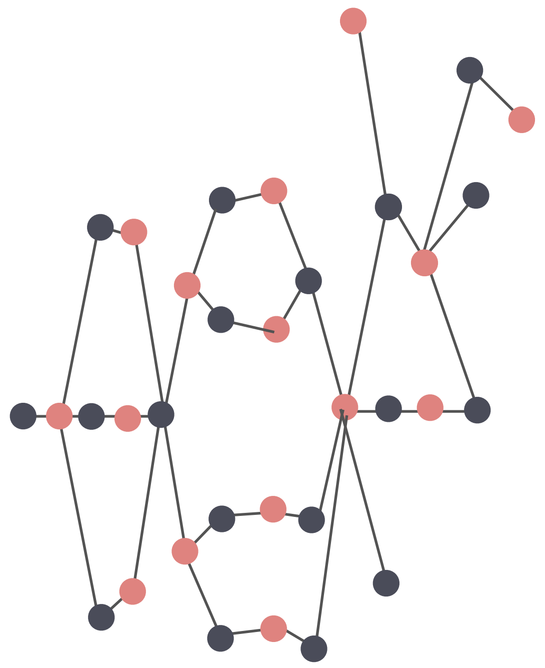
# Overview




Encoding

## Methodology

- Generate large shape dataset
- Identify shape invariant ratios
- Distill complexities into graphs
- Uniformly traverse graphs to decode



Decoding

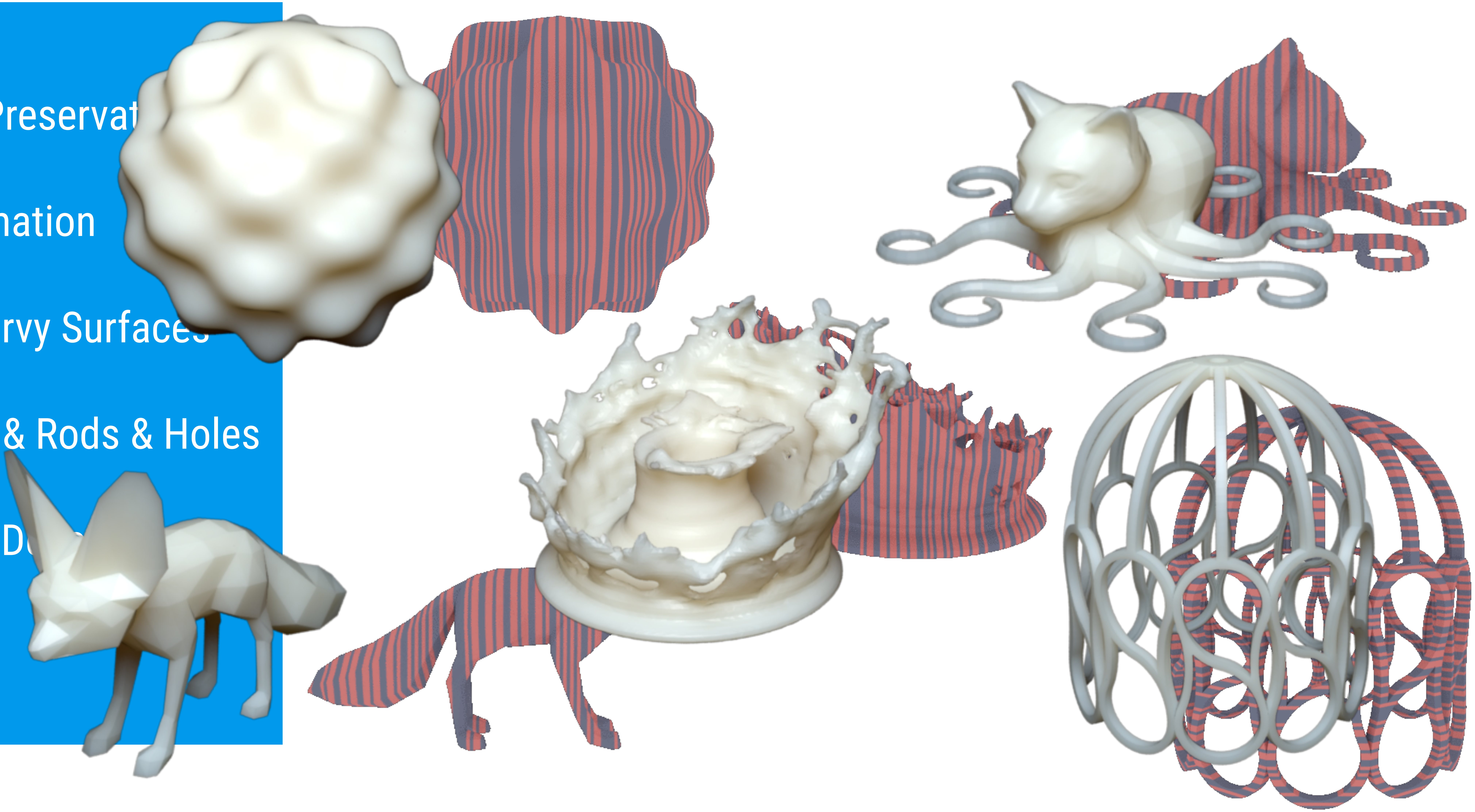
Sample Query Information:

```
#Vertices : 2450
Euler     : 2
Genus     : 1
Closed    : True
Solid     : False
Edge manifold    : True
Duplicated faces : False
```

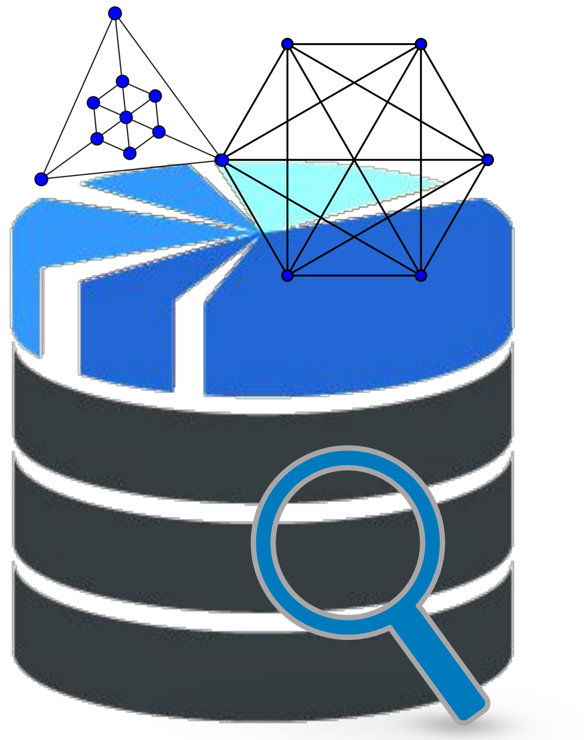
Applications

# Conclusion

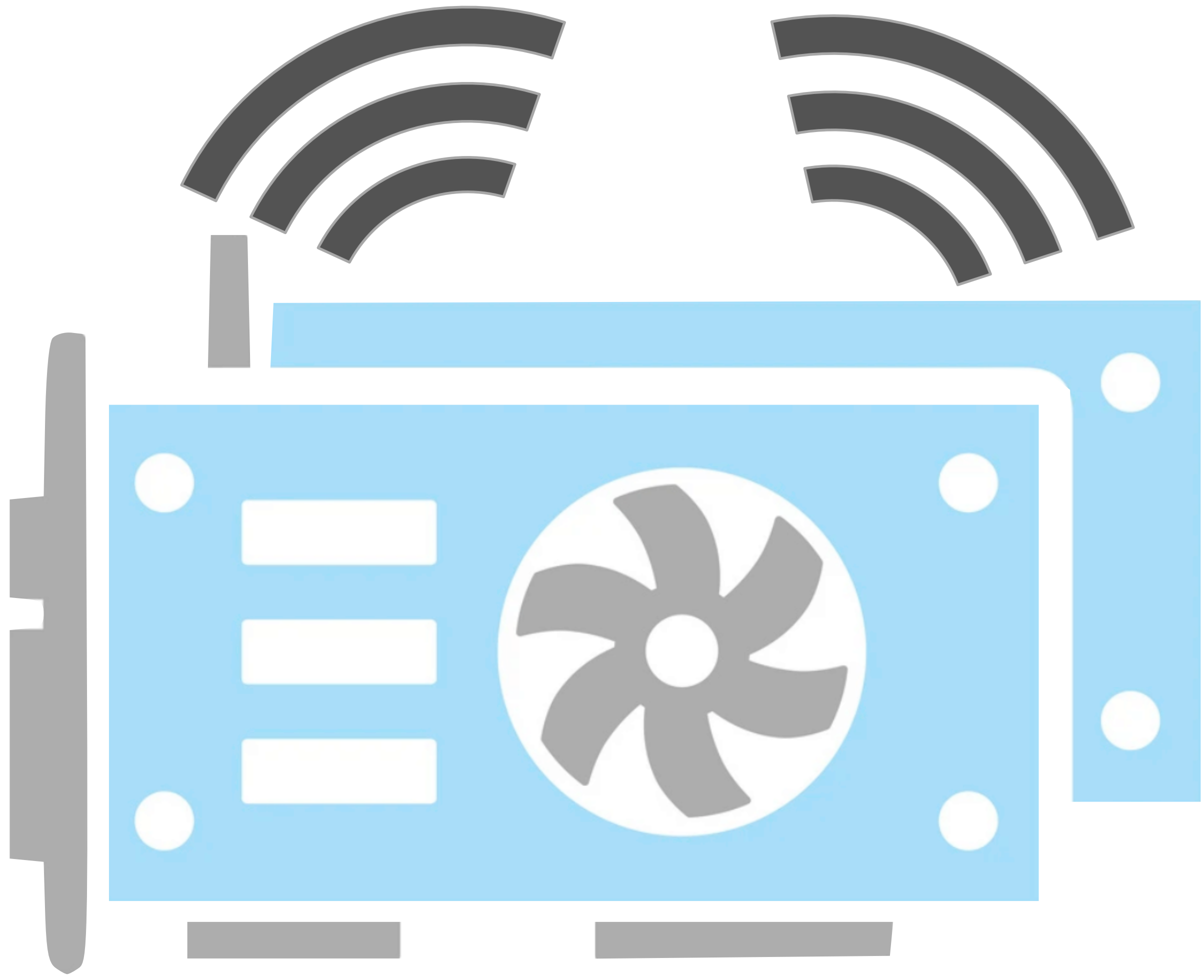
- ✓ Structural Preservat
- ✓ Depth Estimation
- ✓ Rough & Curvy Surfaces
- ✓ Thin Shells & Rods & Holes
- ✓ Accessible D



# Roadmap



Additive Manufacturing



Side-channel Security

Physics-based Contact

# Can one hear the shape of a neural network?:

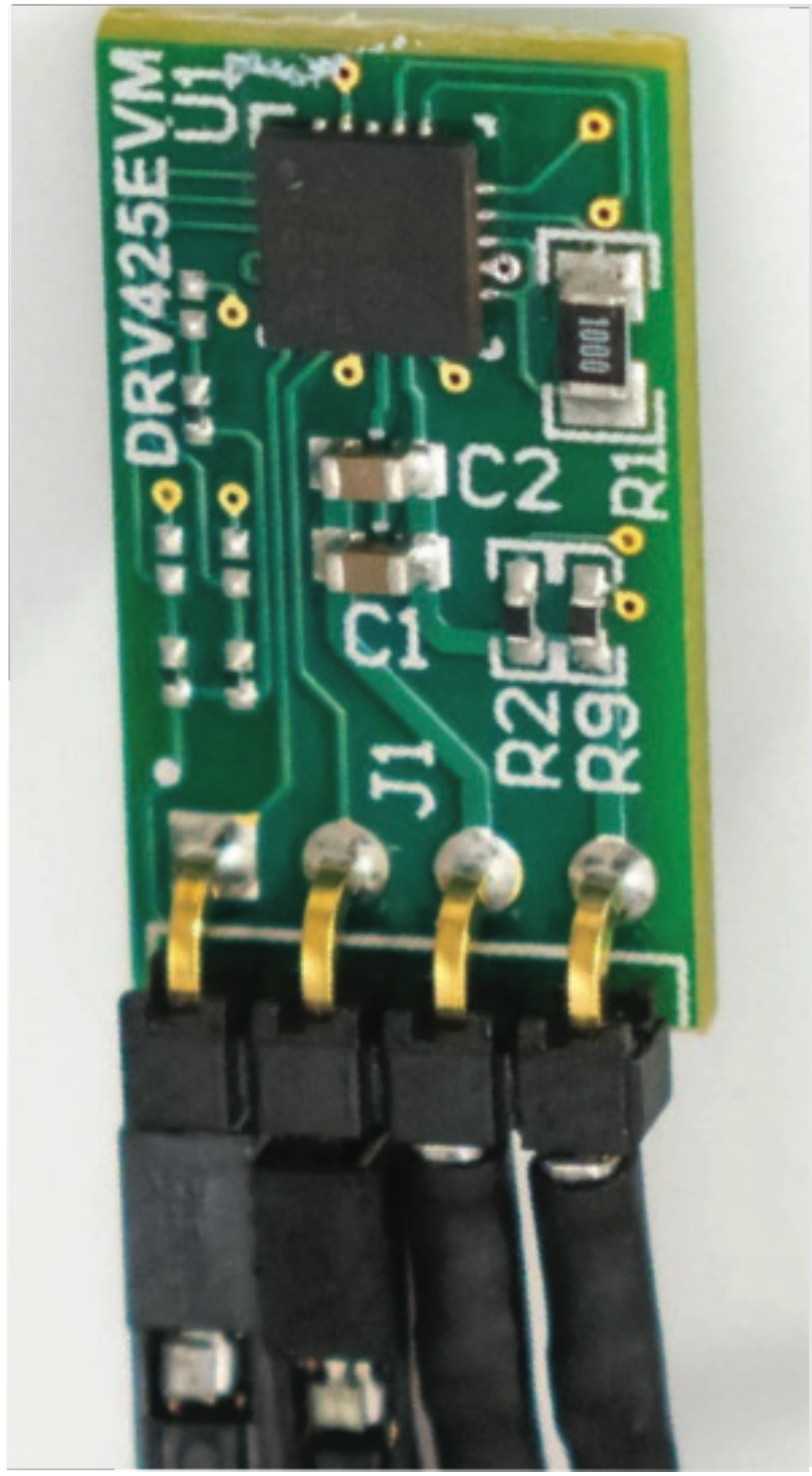
## Snooping the GPU via Magnetic Side Channel


with Chang Xiao, Dingzeyu Li, Eitan Grinspun, Changxi Zheng

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

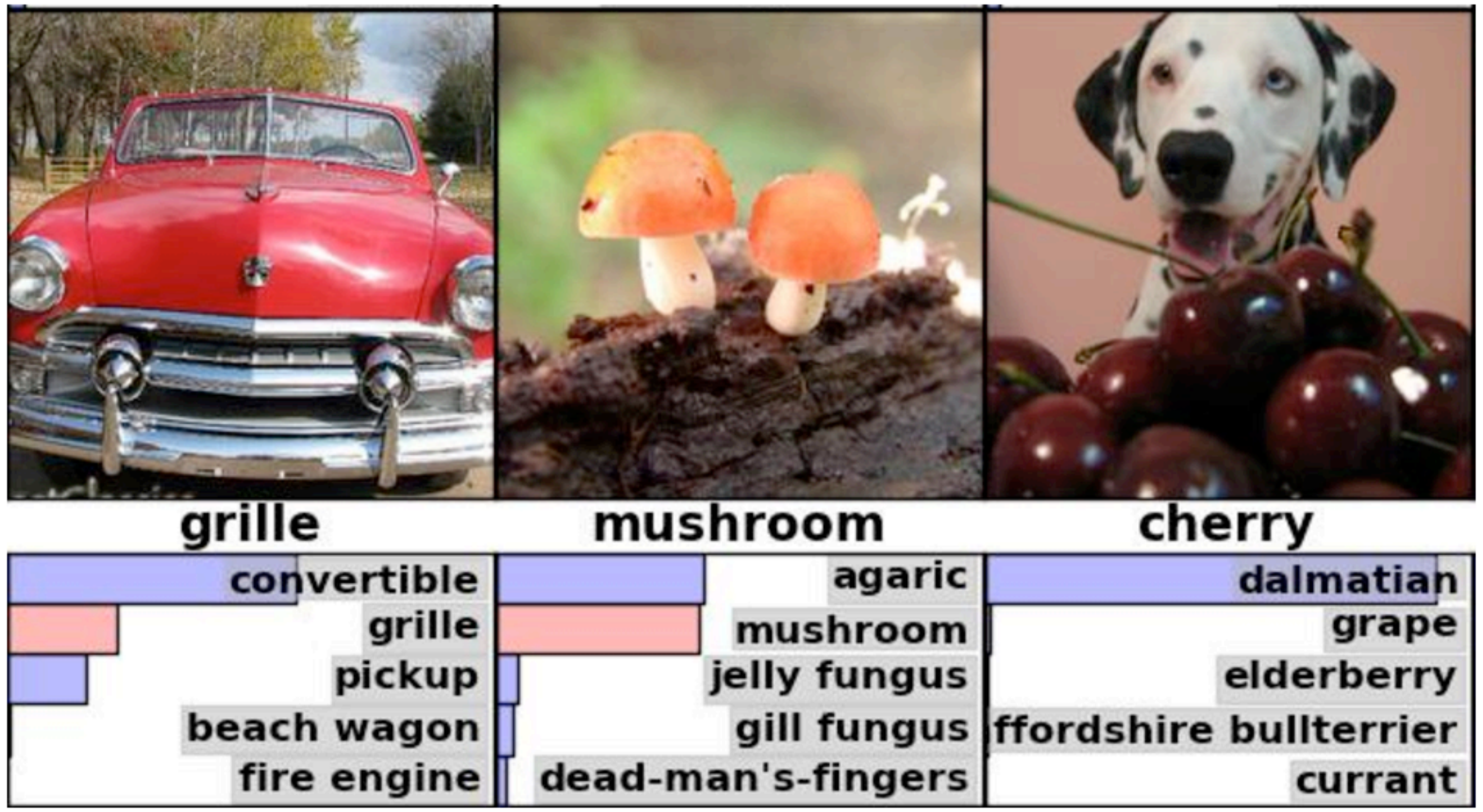
UNIVERSITY OF TORONTO

Adobe

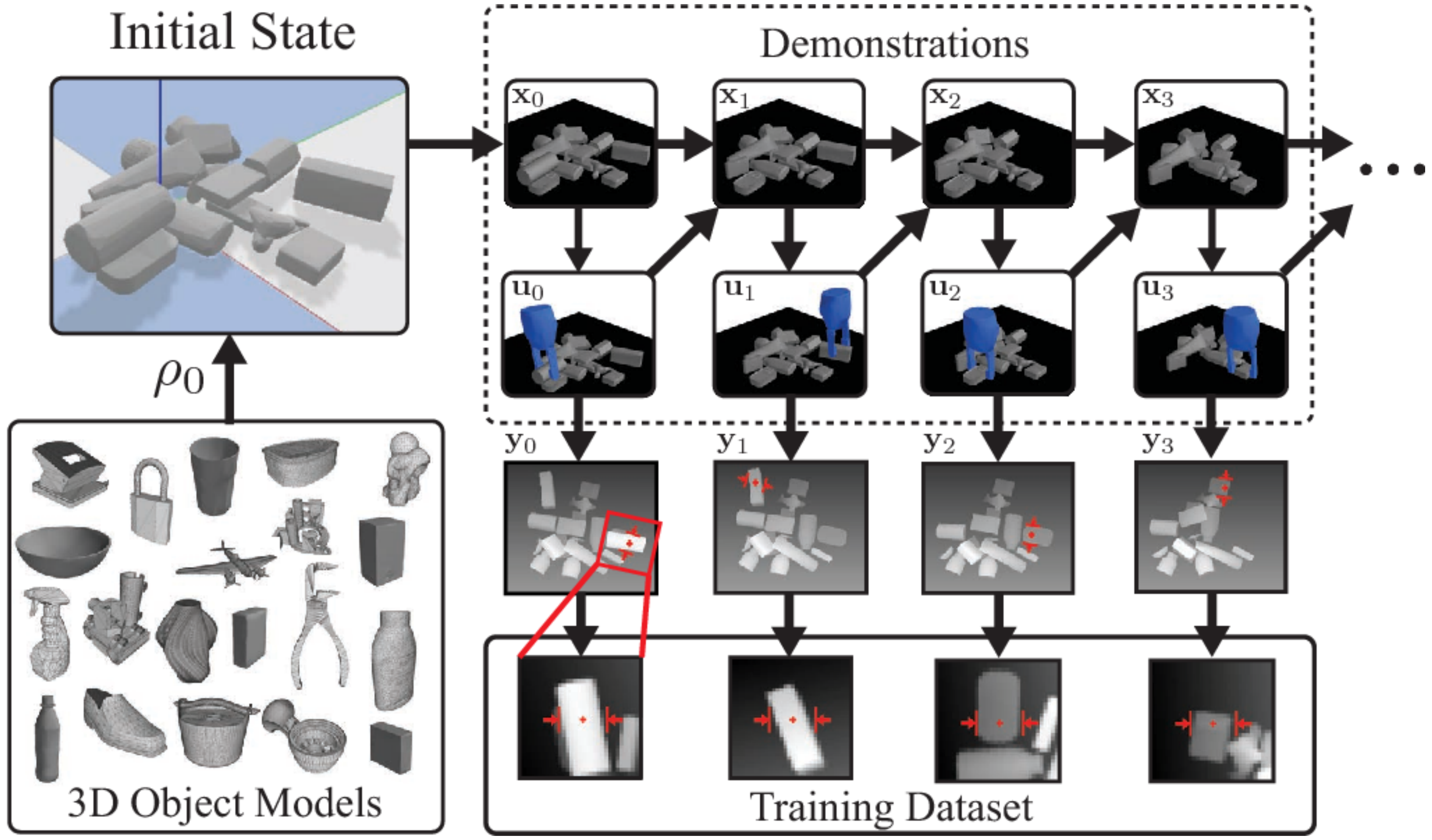
# Neural Supremacy

## Vision



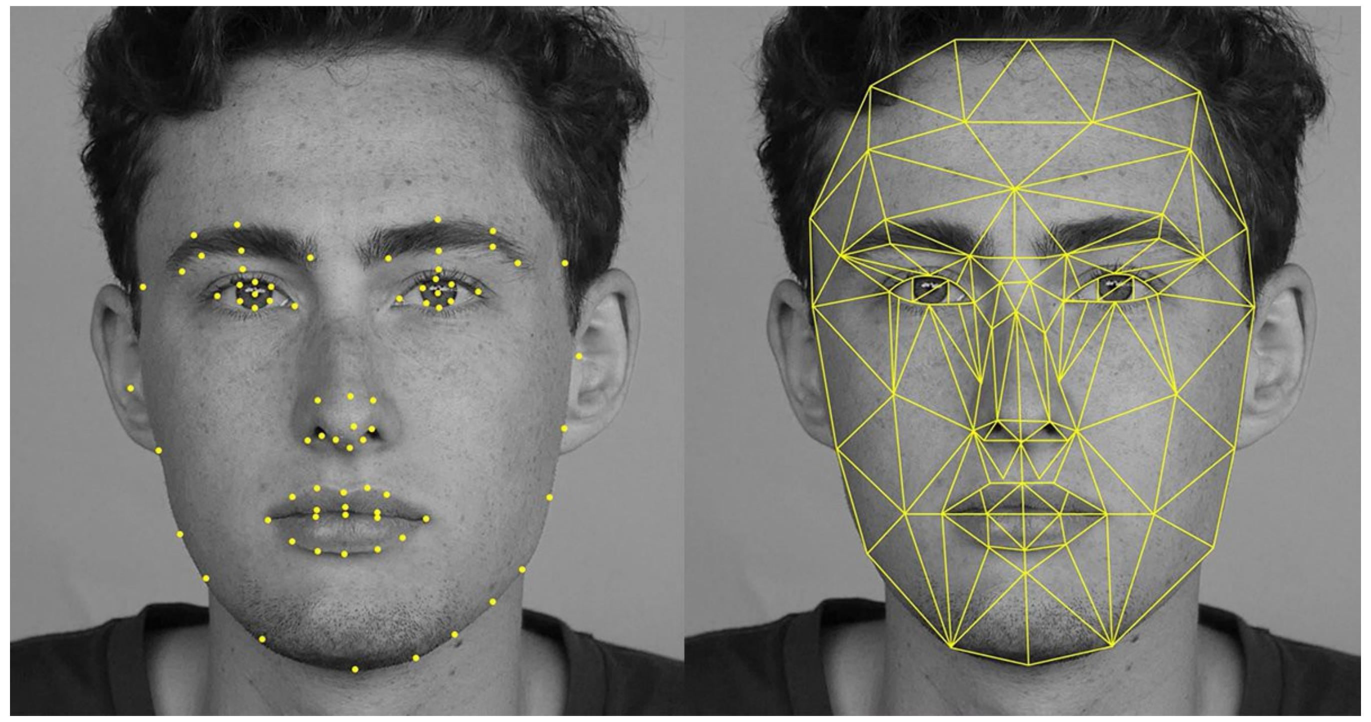

ImageNet Classification with deep convolutional neural networks [Krizhevsky et al. 2012]

## Robotics



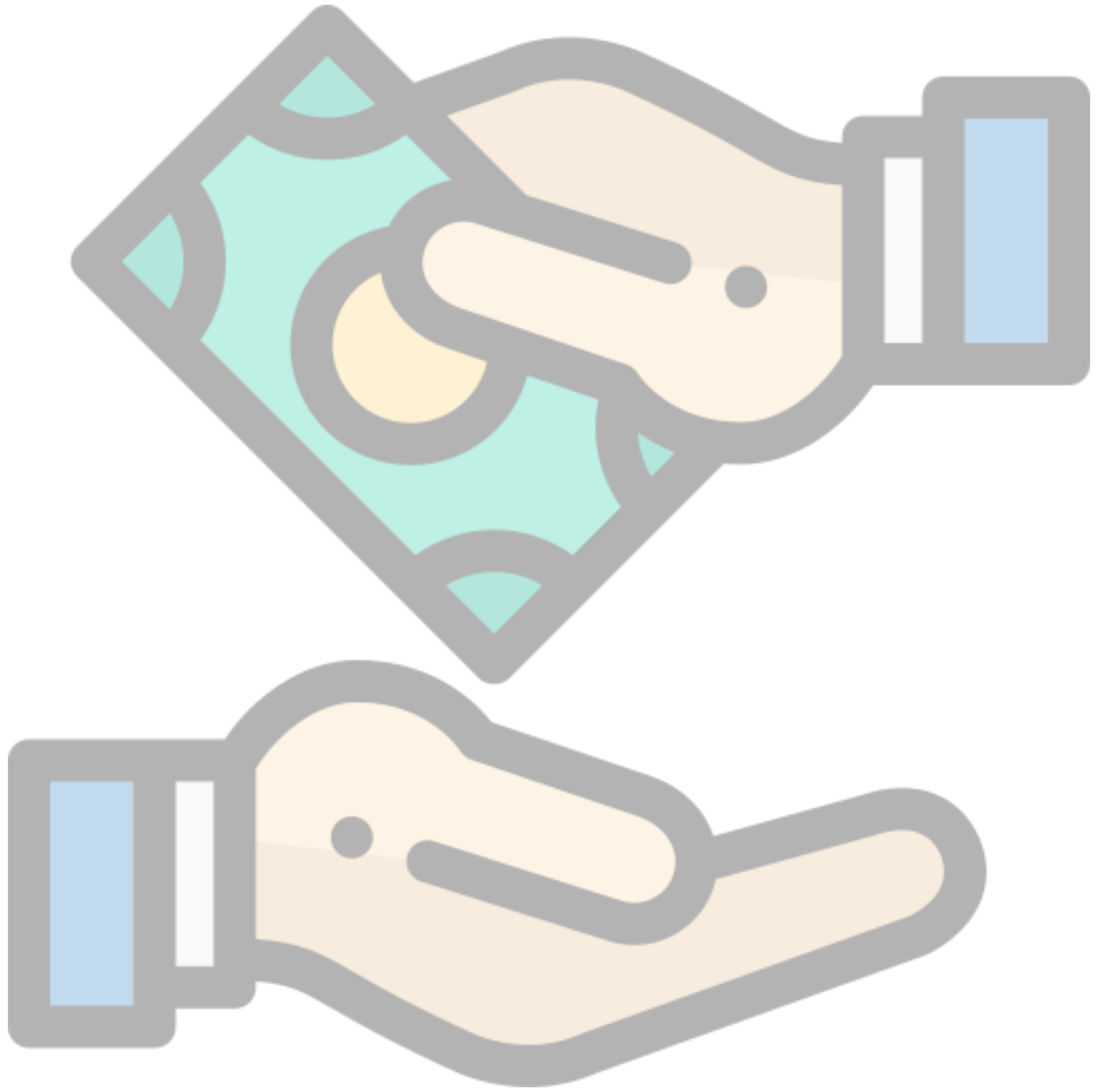

Learning Deep Policies for Robot Bin Picking by Simulating Robust Grasping Sequences [Mahler & Goldberg 2017]

## Security



# Incentives

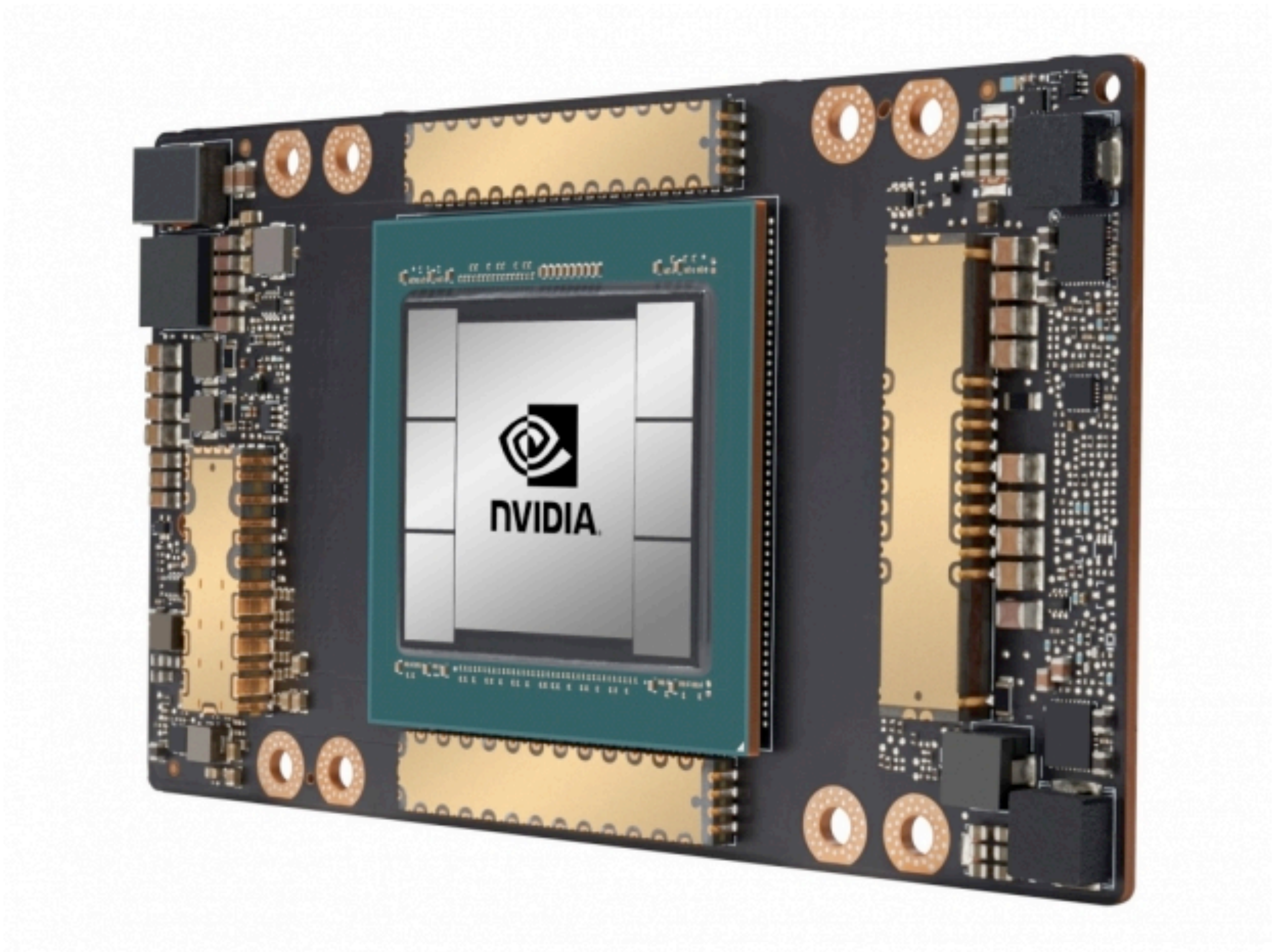

Intellectual Property Theft

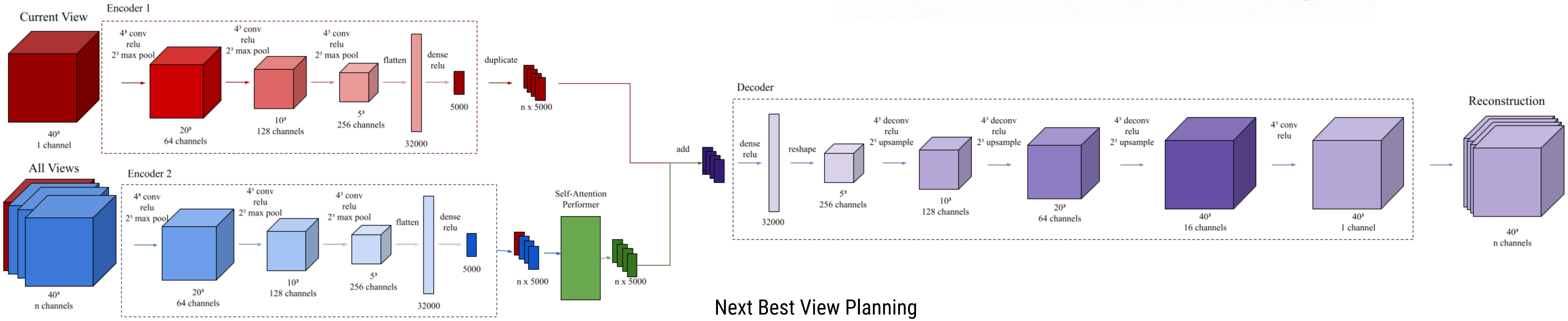


Avoiding Charges


Bypassing Filters

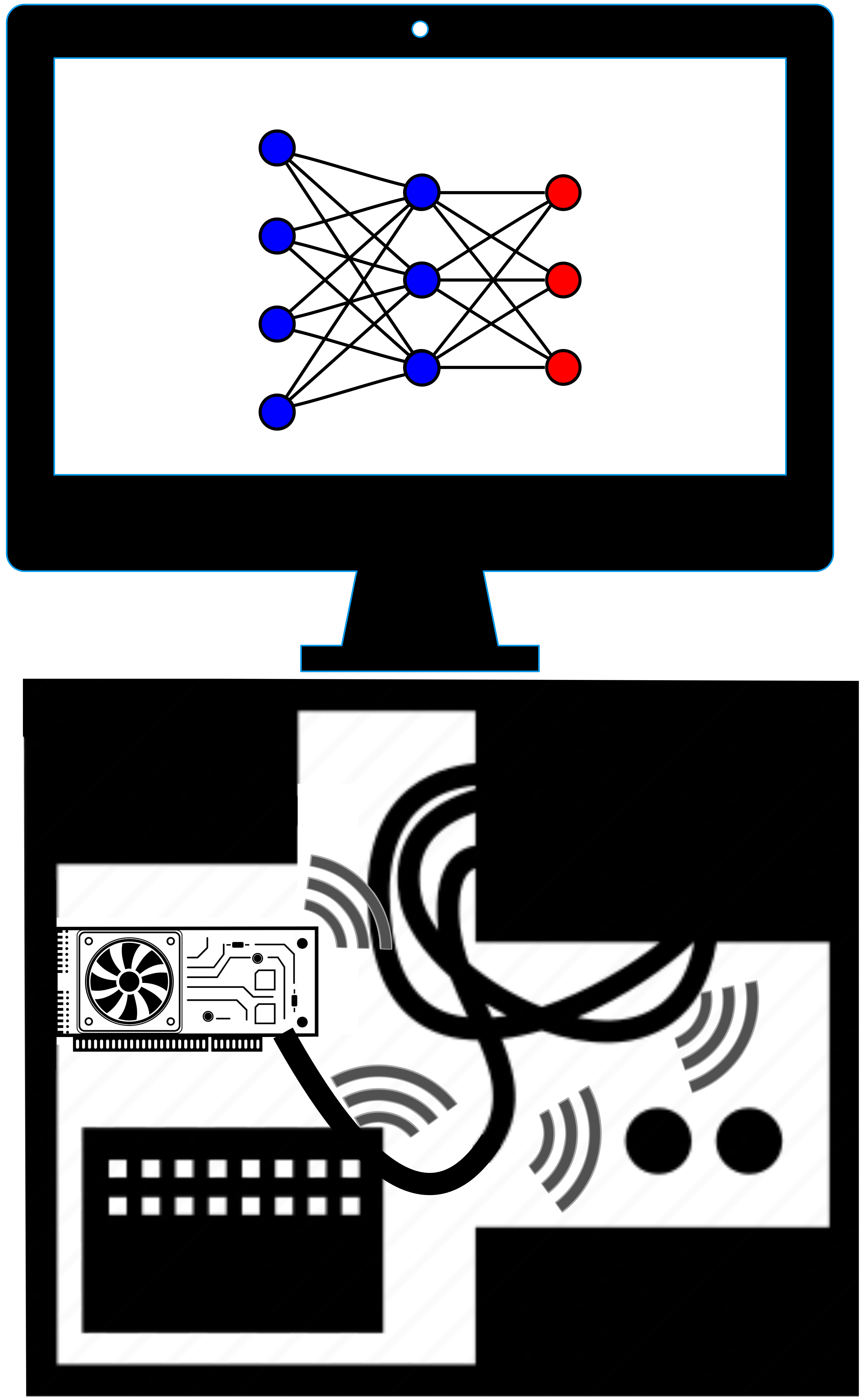
# Machine Learning ❤ GPUs

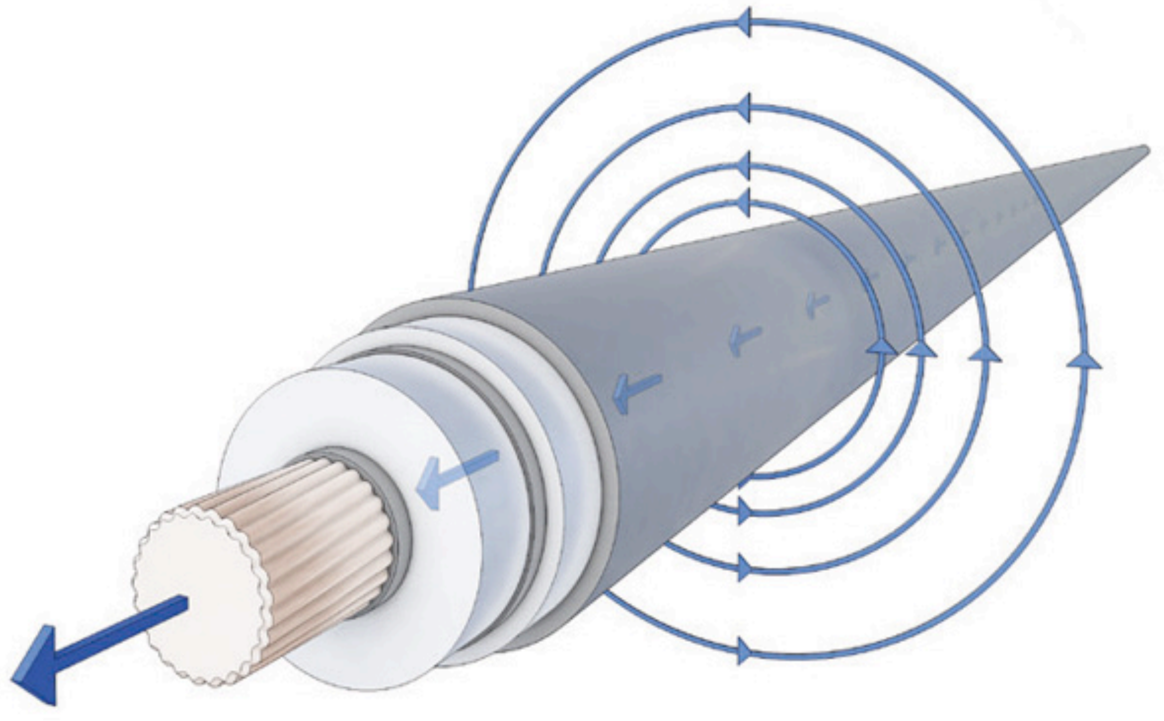

Next Best View Planning
[Watkins-Valls et al. 2021]

# Physical Backdoor



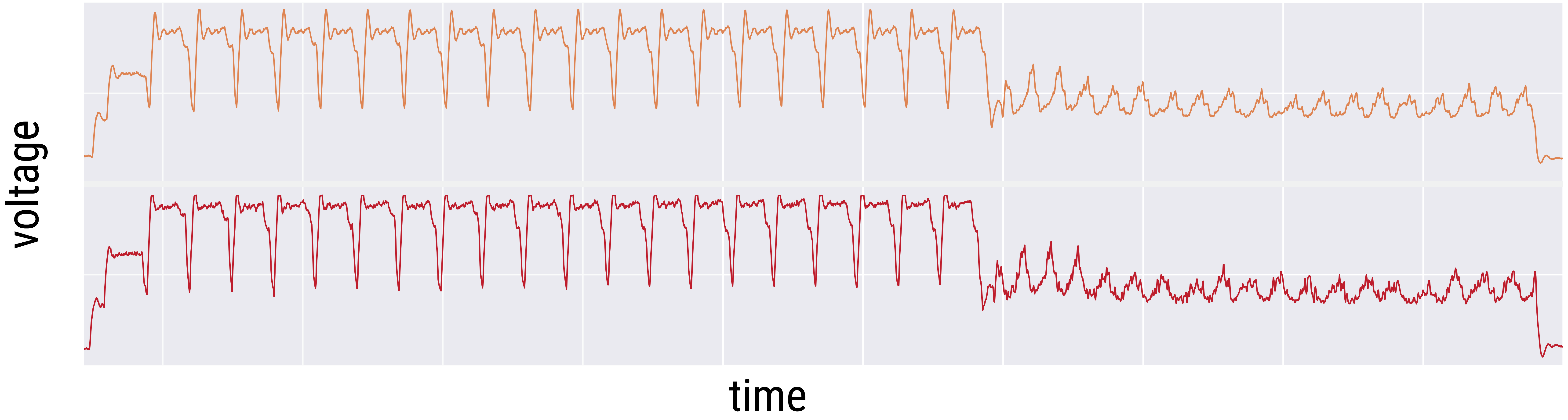
$$\nabla \times \mathbf{B} = \mu_0 \left( \mathbf{J} + \varepsilon_0 \frac{\partial \mathbf{E}}{\partial t} \right)$$

Ampere-Maxwell

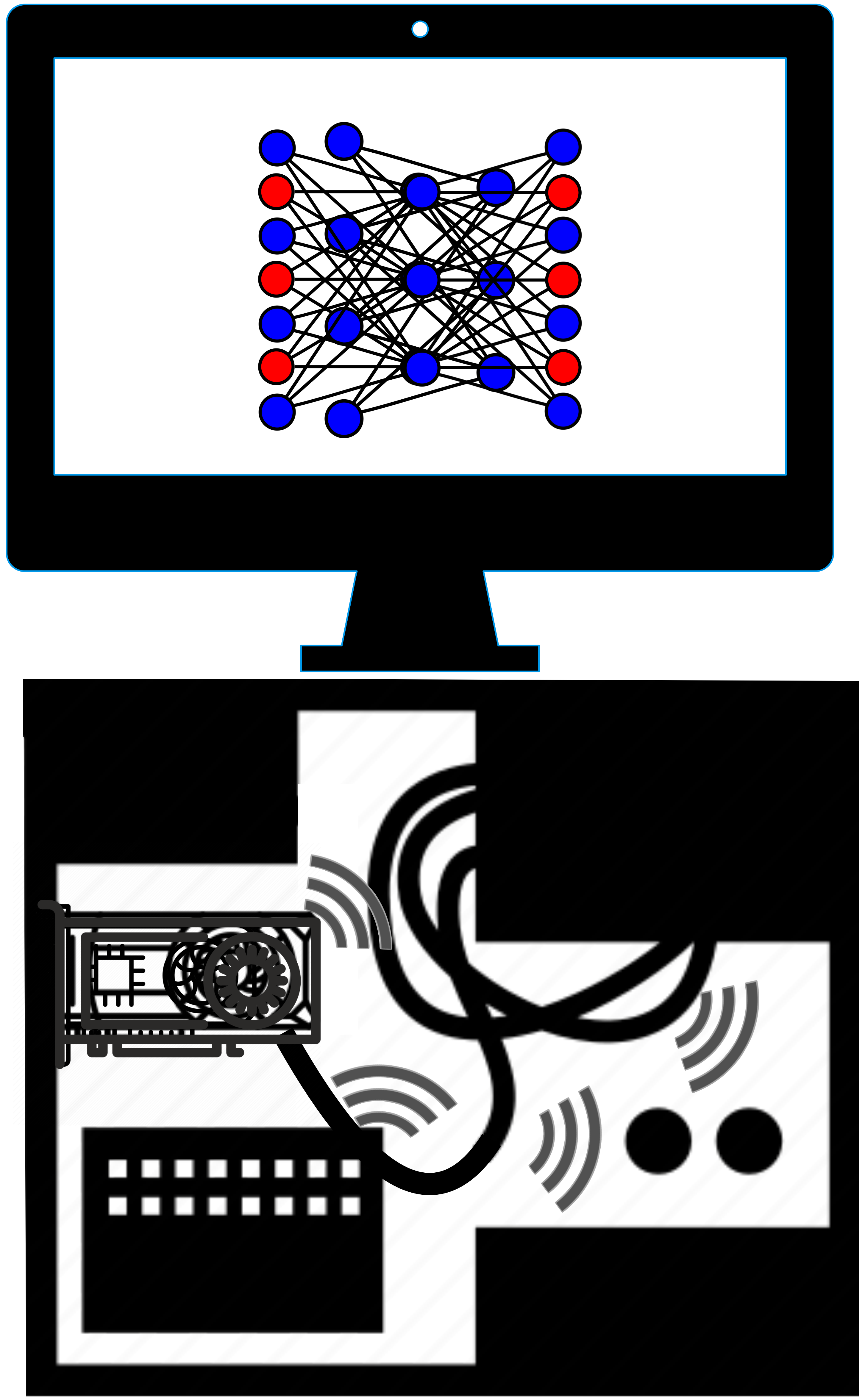


$$B = \frac{\mu_0 N I}{2R}$$

Biot-Savart

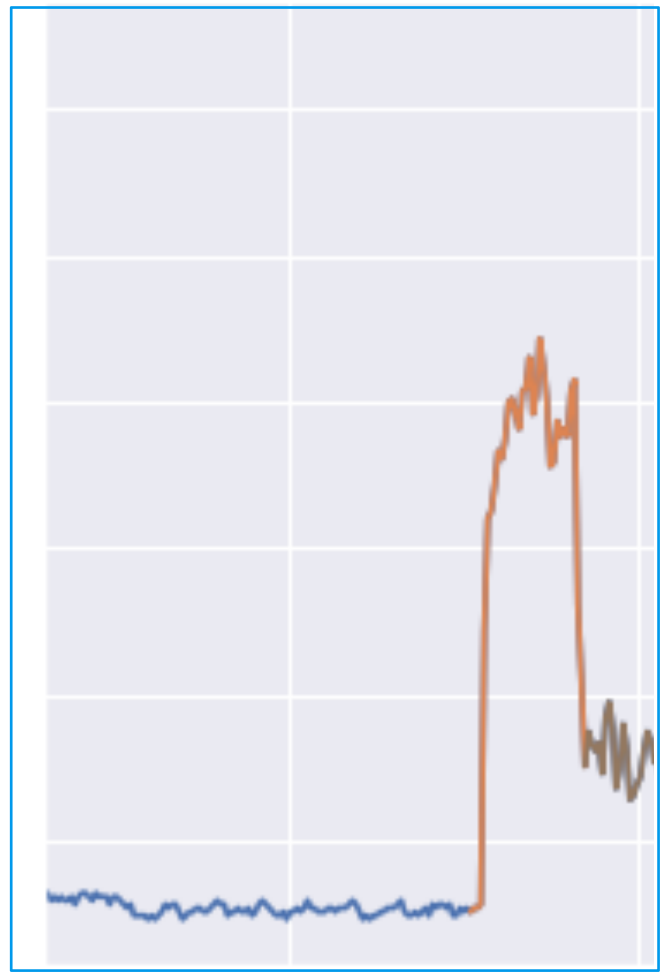


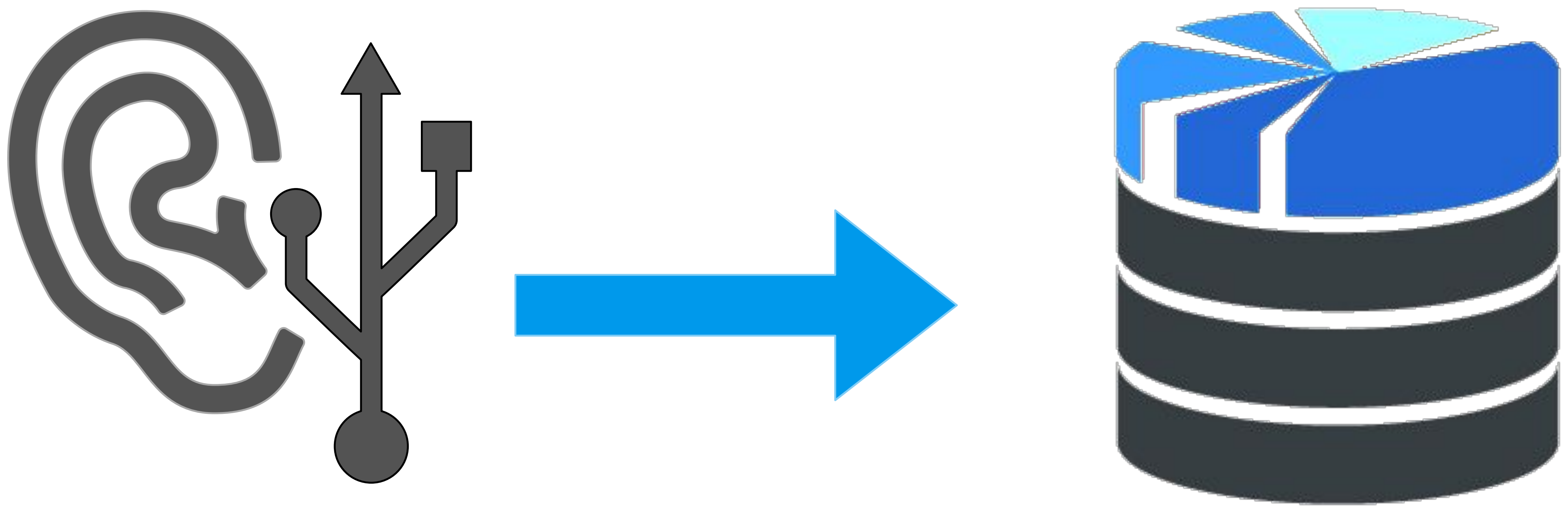
# GPU Inference Traces



Methodology:

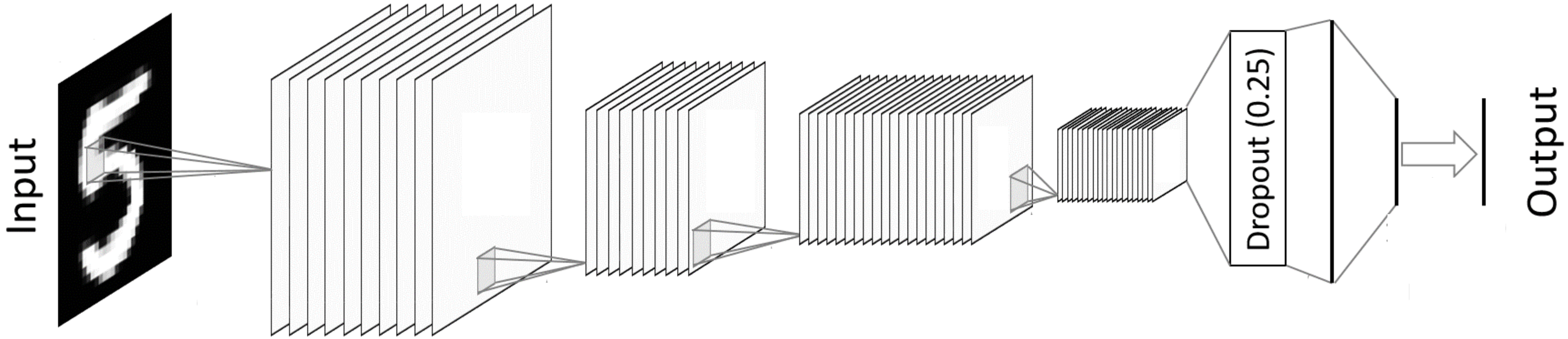
- ➡Generate dataset
- ➡Identify nodes in signal
- ➡Assemble graphs
- ➡Optimize for parameters





# Target Scope

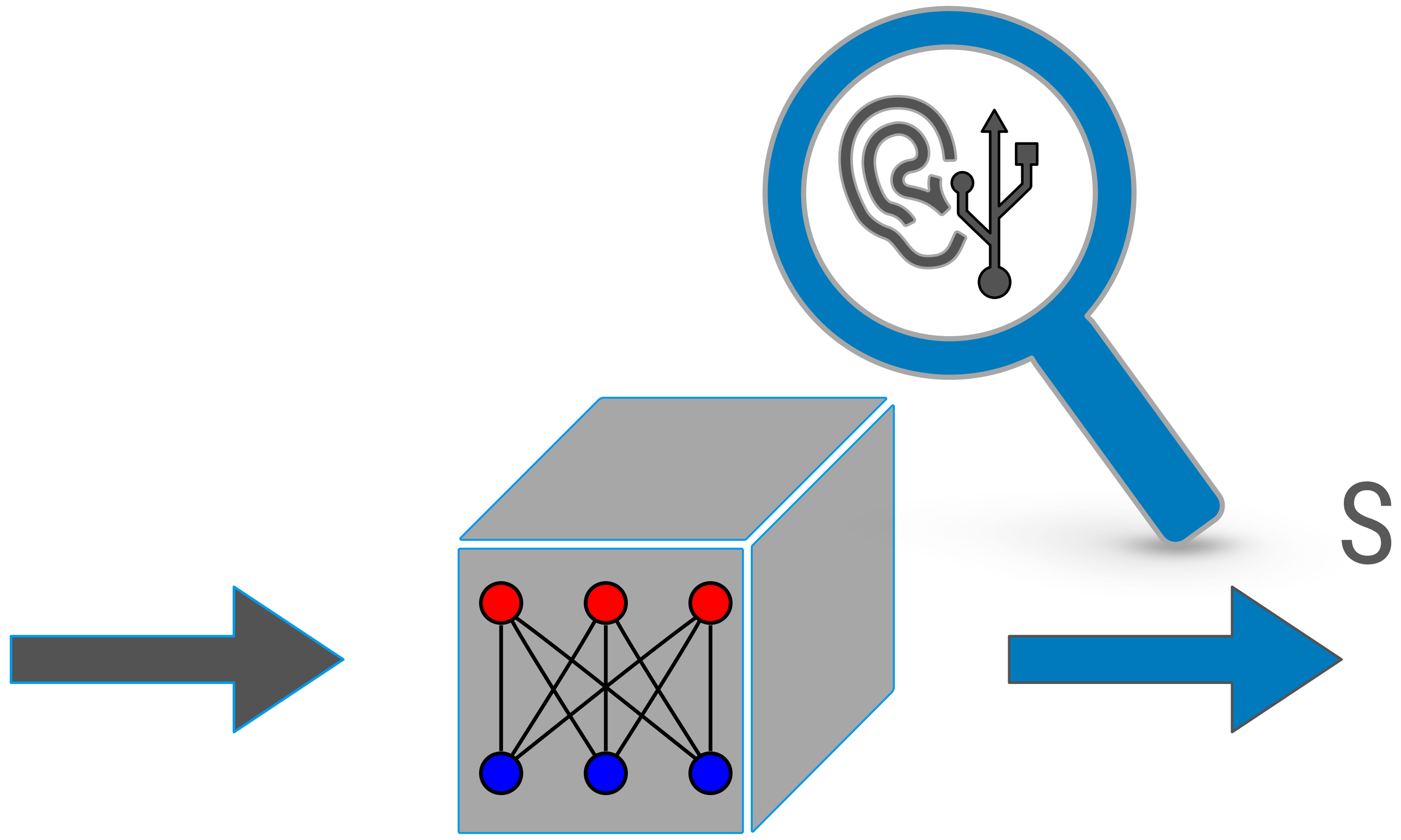
➡Order
➡Type
➡Width
➡Parameters



# Attacker's Capability

Known size

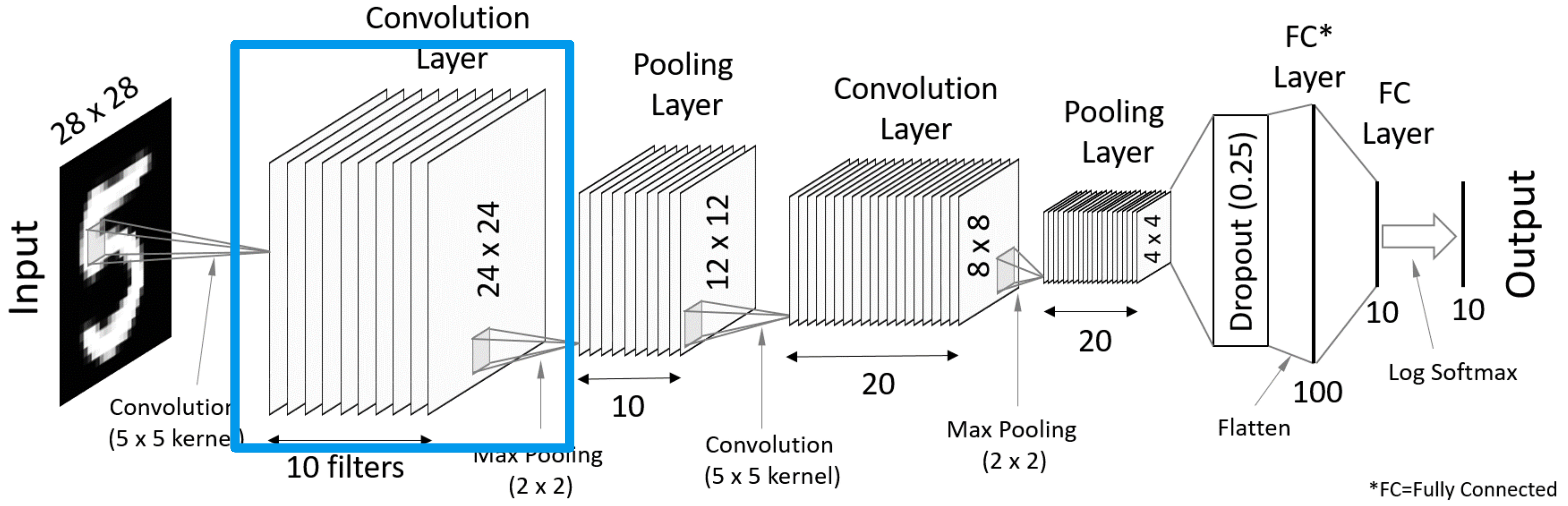
input image



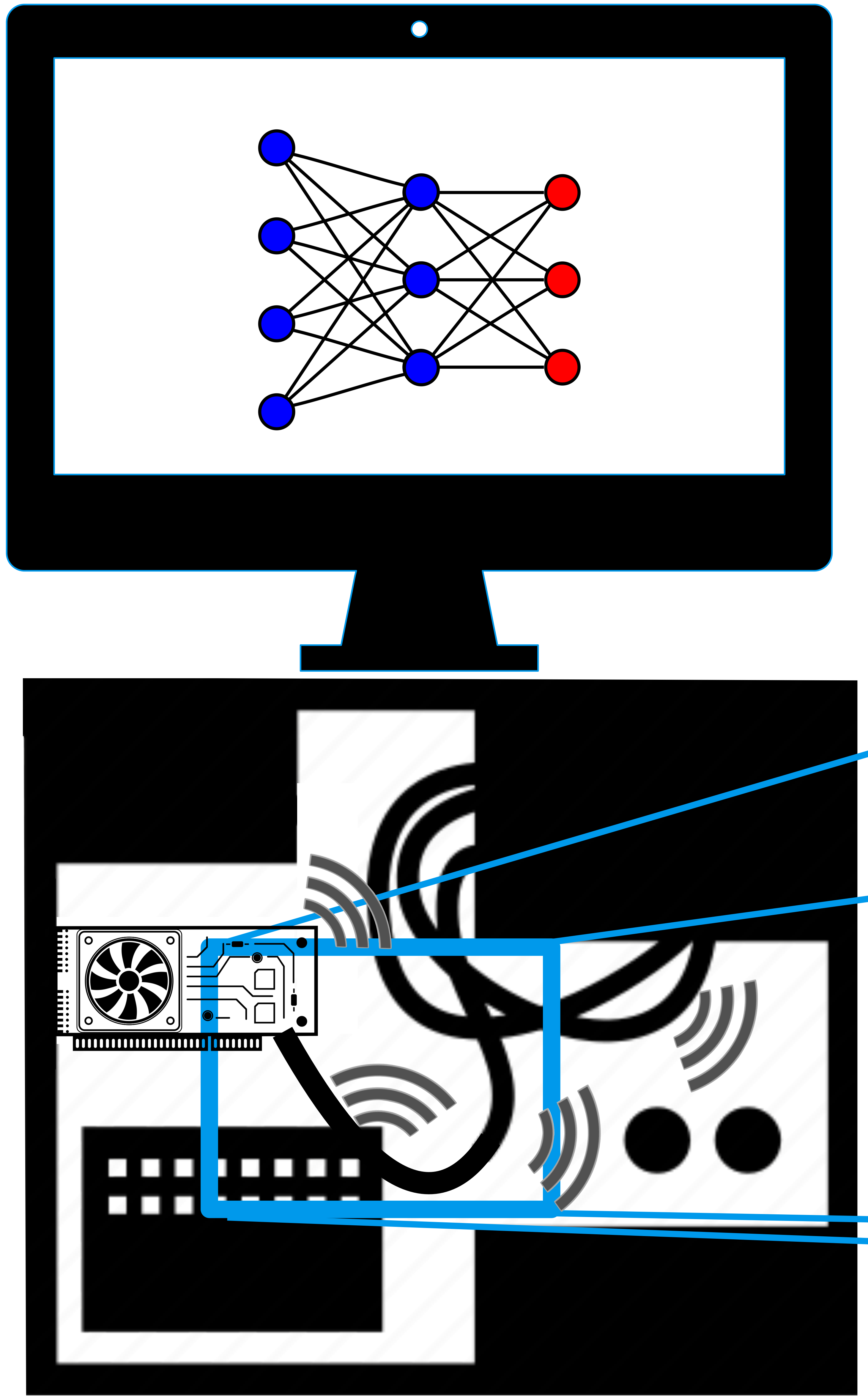
Side-channel

EM signal

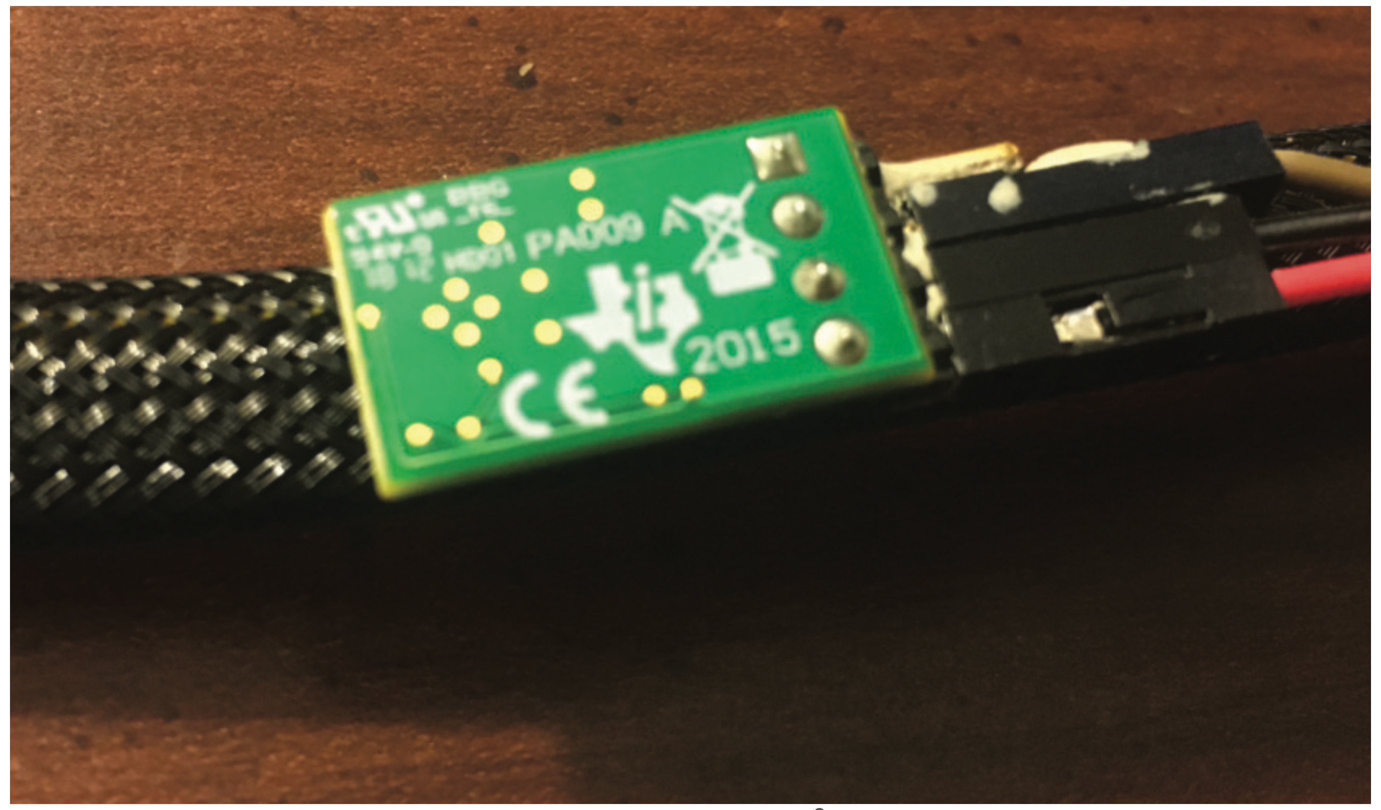
# Layer-by-Layer Computation



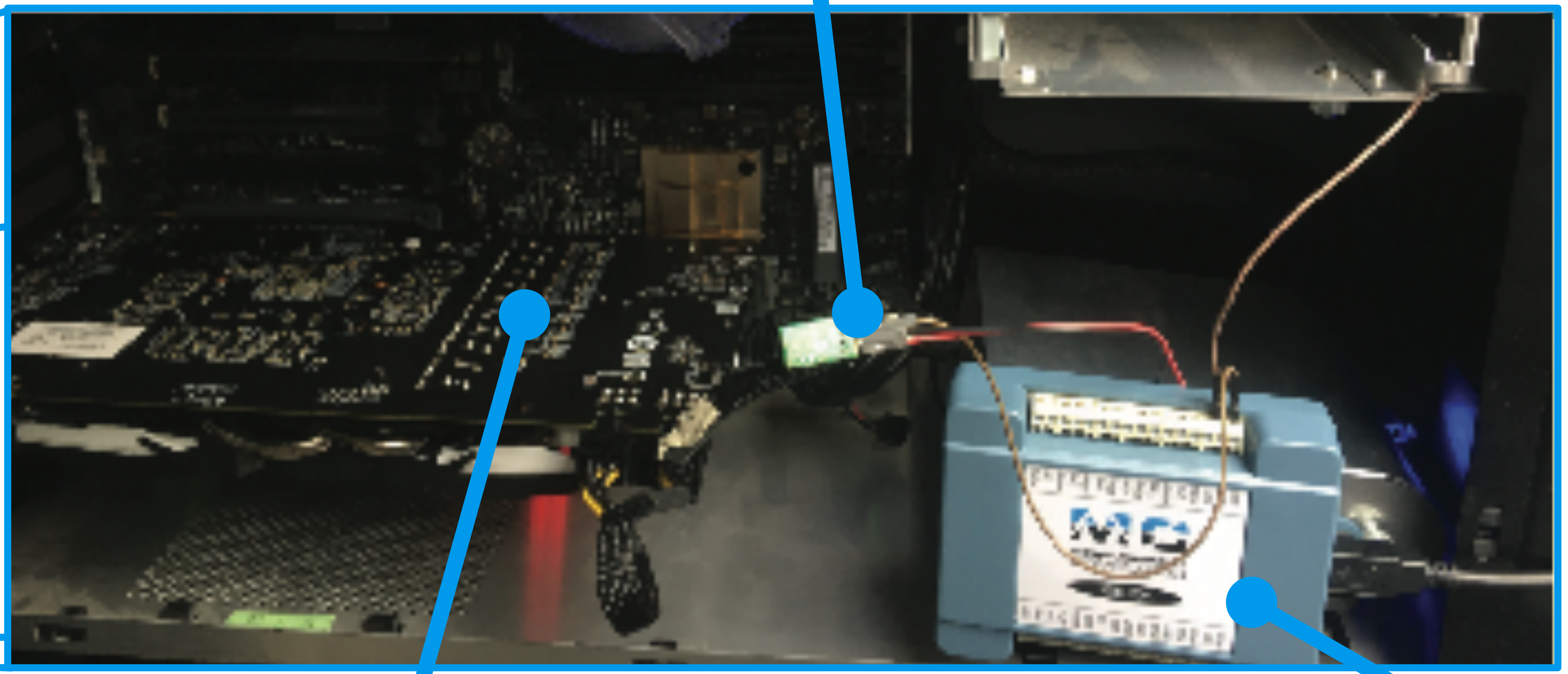
# Sensor Setup



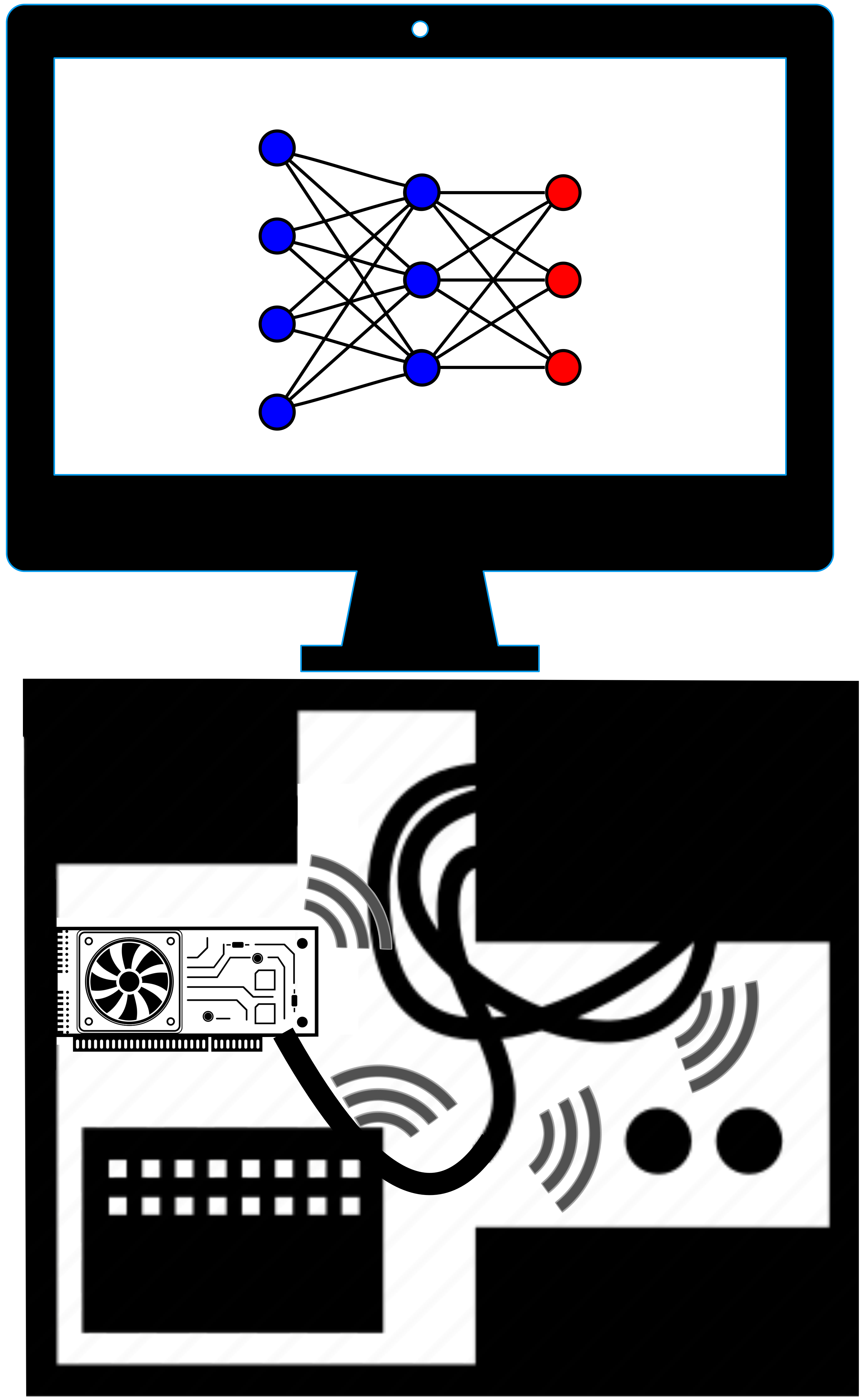
side view

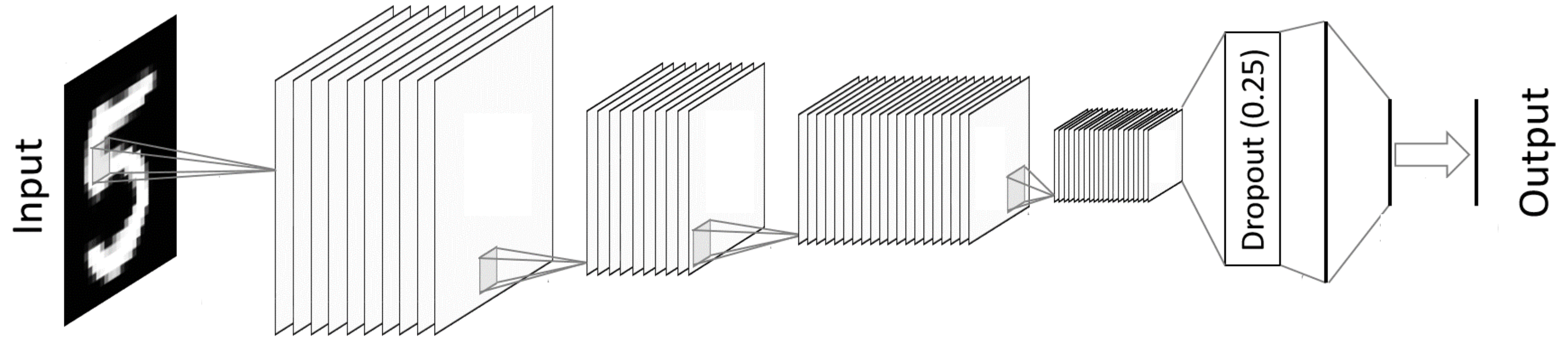


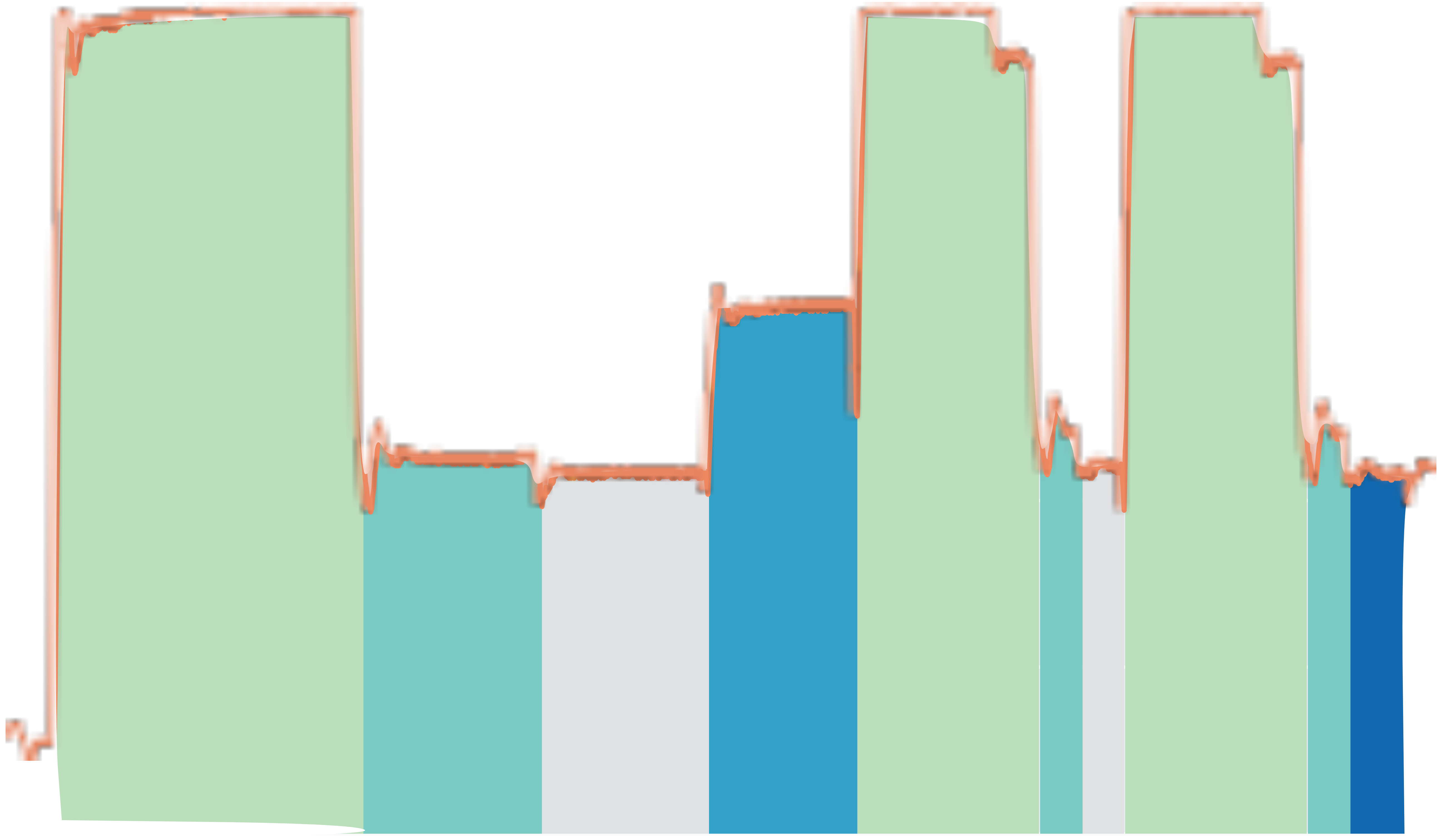
top view



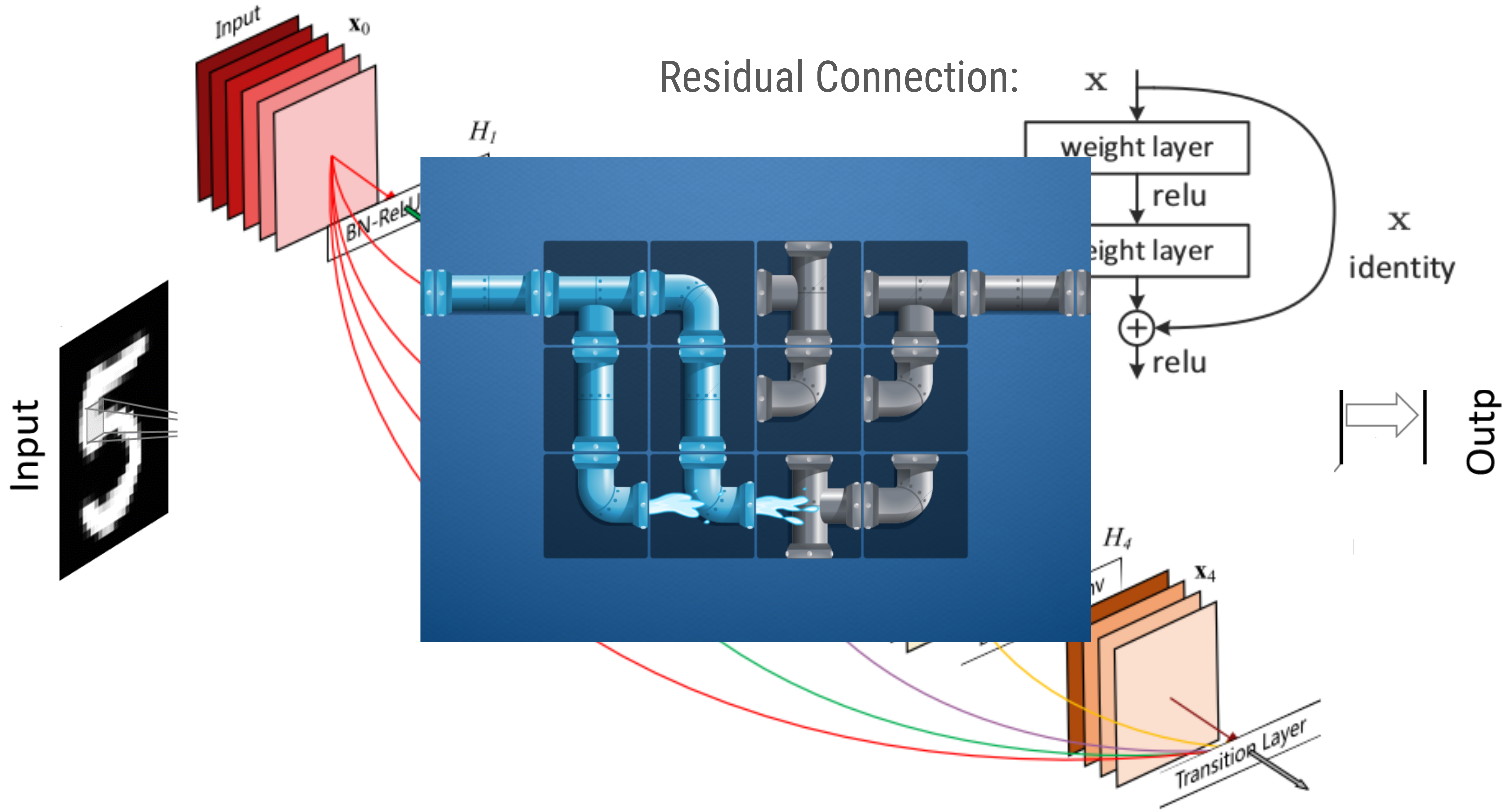
# Signal Classification



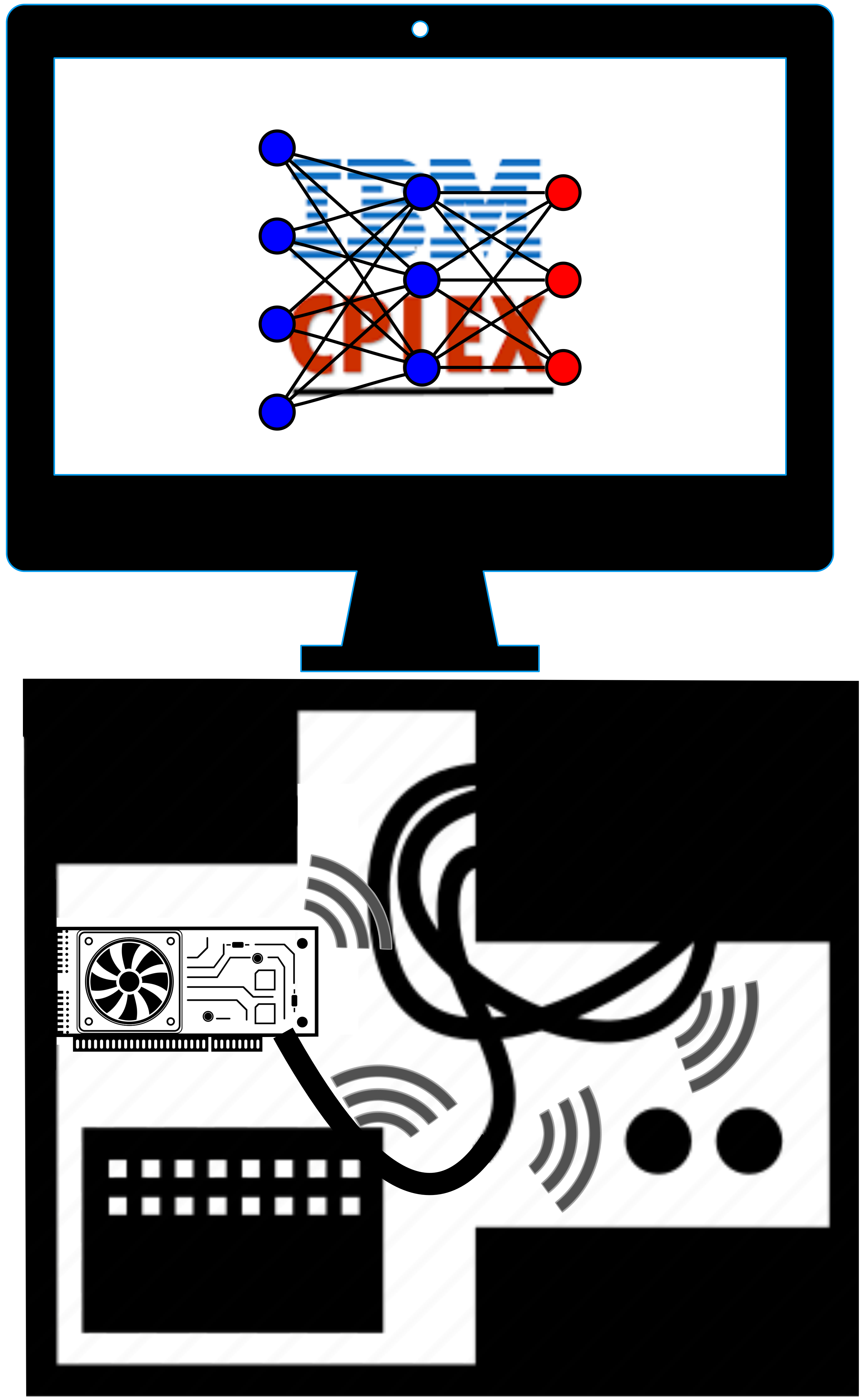


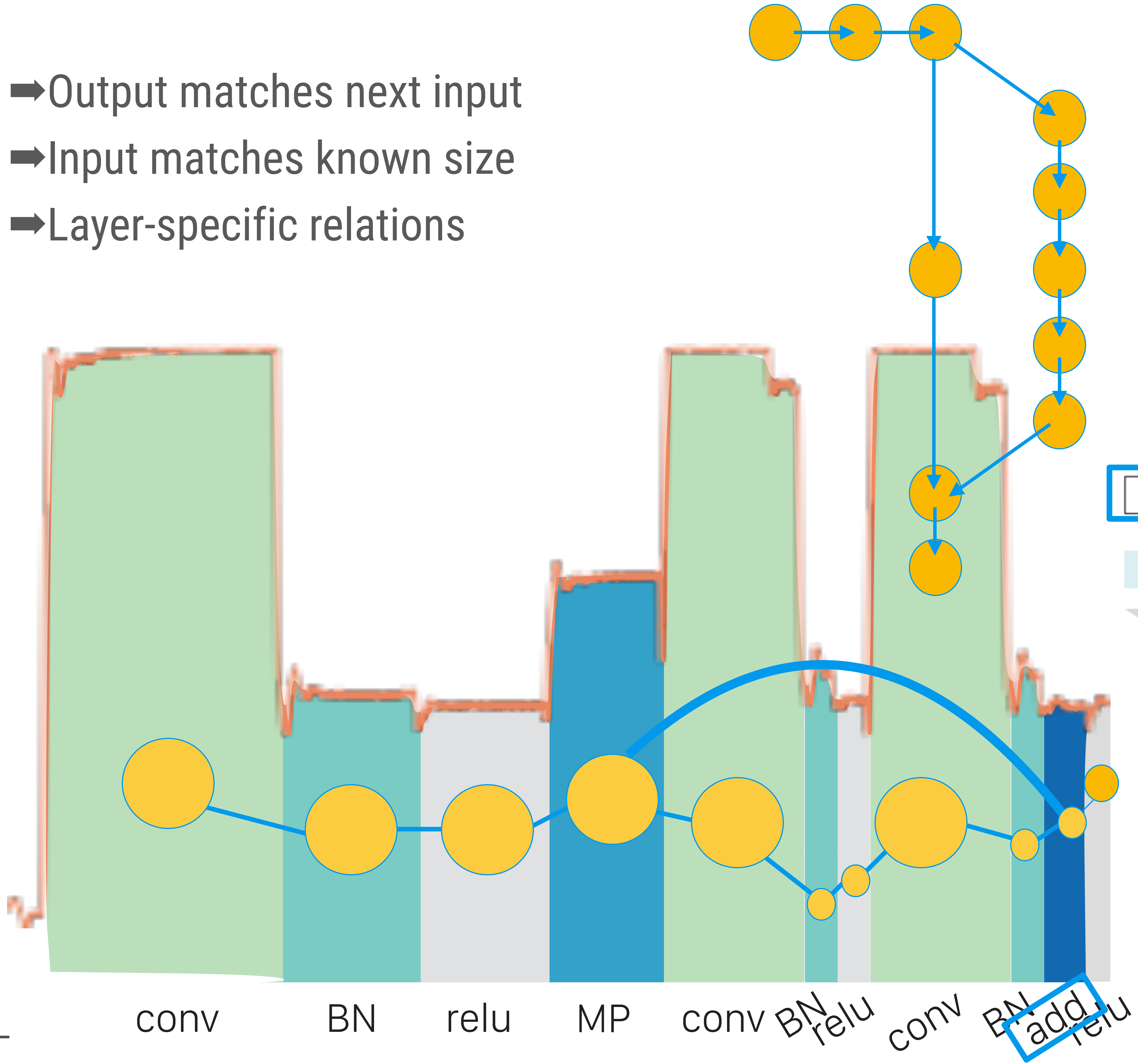
# Consistency flow

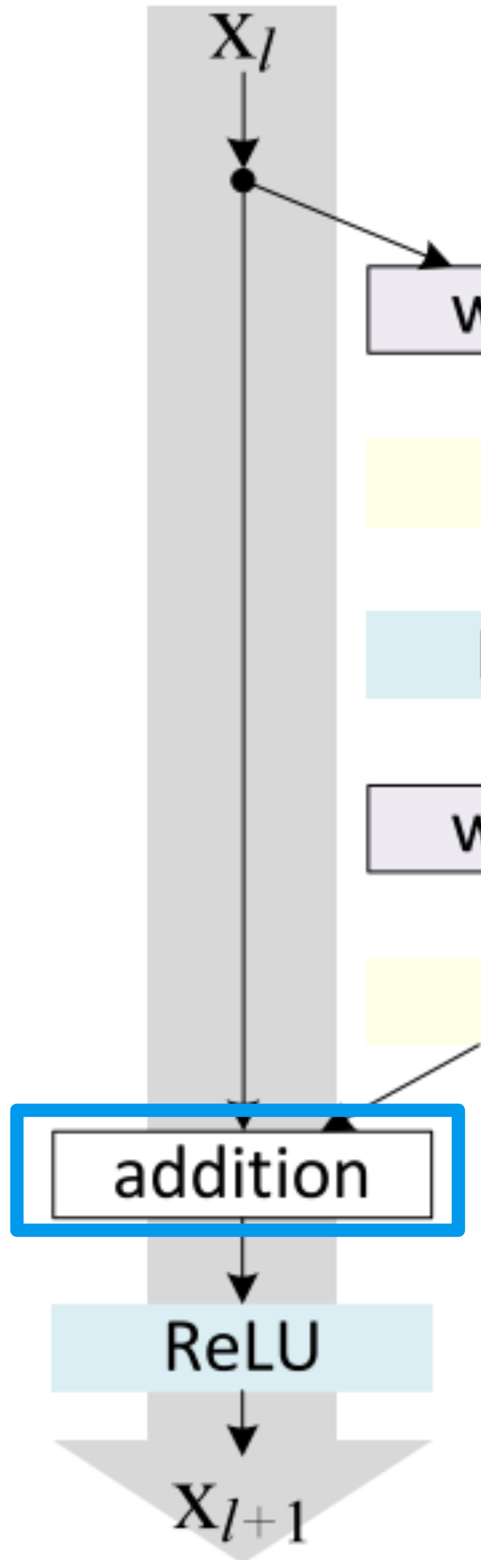


# Optimizing over Graphs




➡Output matches next input
➡Input matches known size
➡Layer-specific relations

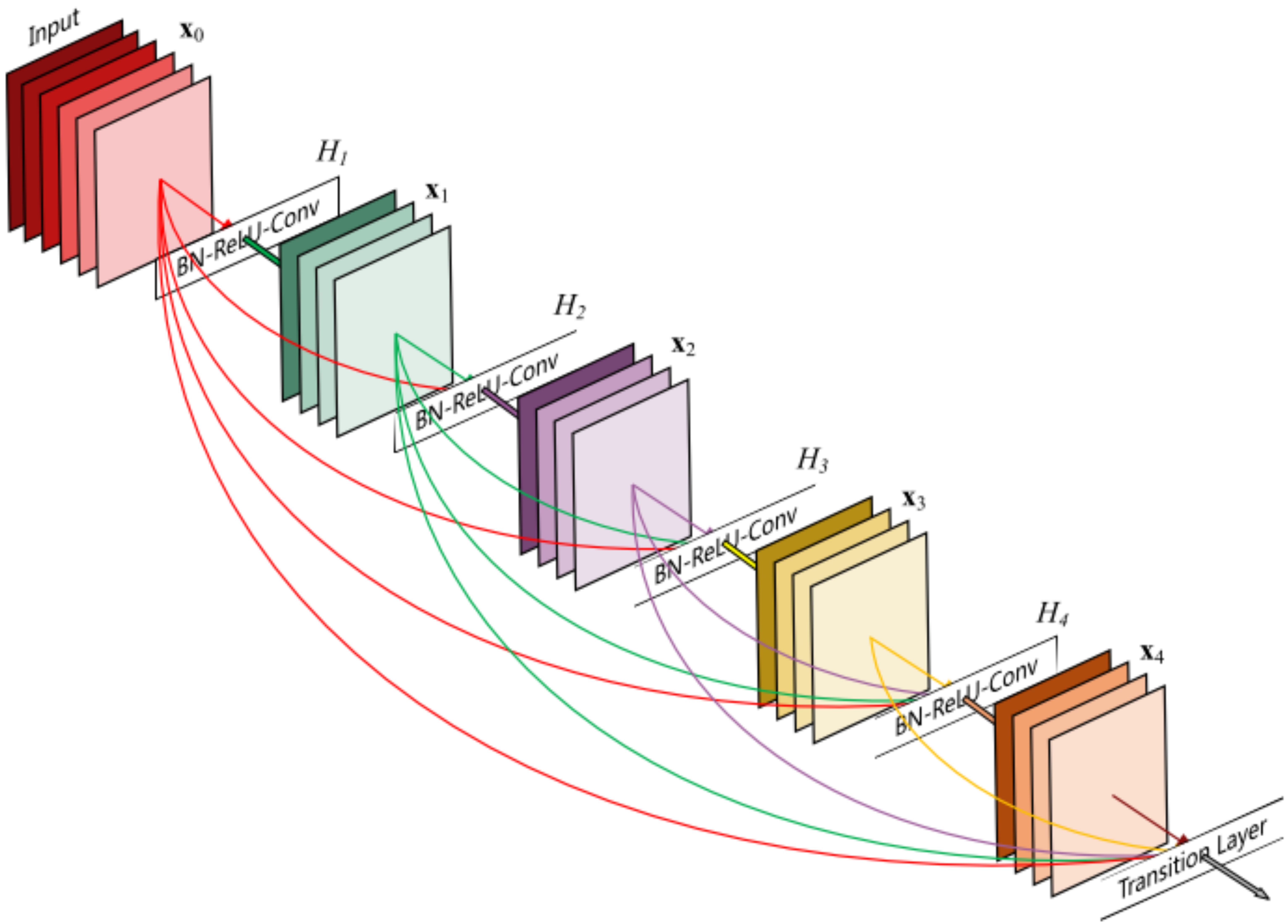


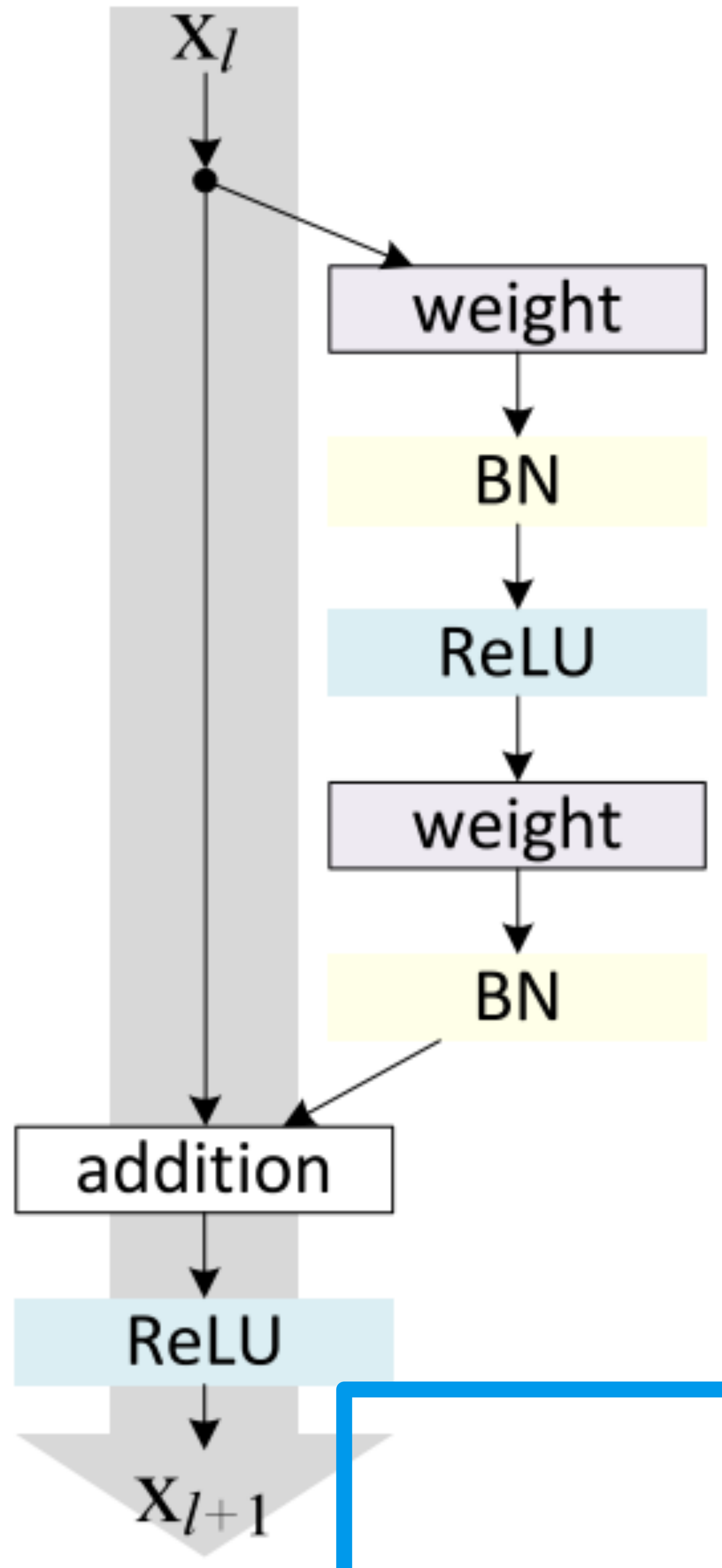




ResNet

Residual Block

# Neural Graphs



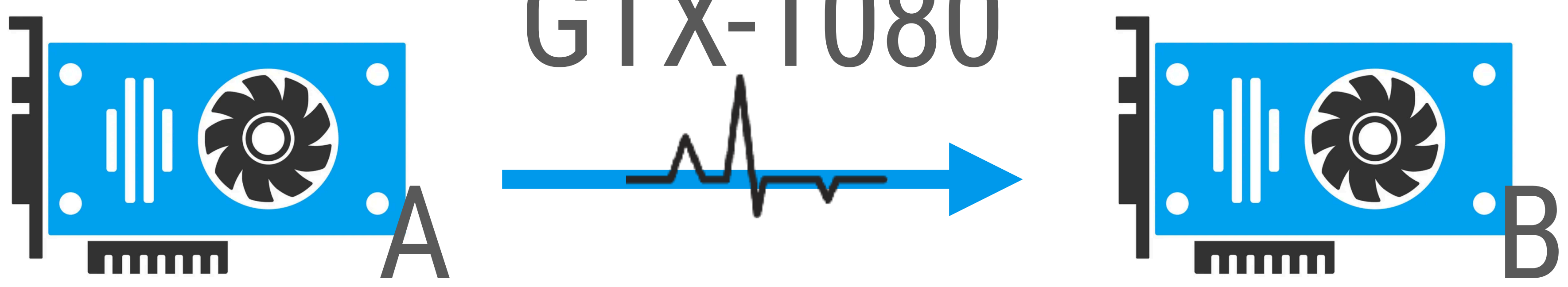
# Topology Reconstruction

| Layer Type | Prec. | Rec. | F1 | # samples |
|---|---|---|---|---|
| LSTM | .997 | .992 | .995 | 8,704 |
| Conv | .993 | .996 | .994 | 447,968 |
| Fully-connected | .901 | .796 | .846 | 10,783 |
| Add | .984 | .994 | .989 | 22,714 |
| BatchNorm | .953 | .955 | .954 | 47,440 |
| MaxPool | .957 | .697 | .806 | 4,045 |
| AvgPool | .371 | .760 | .499 | 675 |
| ReLU | .861 | .967 | .911 | 28,512 |
| ELU | .464 | .825 | .594 | 2,834 |
| LeakyReLU | .732 | .578 | .646 | 9,410 |
| Sigmoid | .694 | .511 | .588 | 8,744 |
| Tanh | .773 | .557 | .648 | 4,832 |
| Weighted Avg. | **.968** | **.967** | **.966** | - |

Titan V

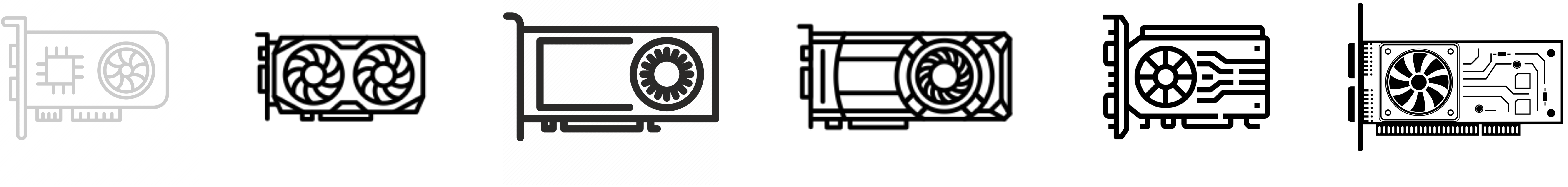
| | Prec. | Rec. | F1 | # samples |
|---|---|---|---|---|
| LSTM | .997 | .999 | .998 | 12,186 |
| Conv | .985 | .989 | .987 | 141,164 |
| Fully-connected | .818 | .969 | .887 | 9,301 |
| Add | .962 | .941 | .951 | 30,214 |
| BatchNorm | .956 | .944 | .950 | 48,433 |
| MaxPool | .809 | .701 | .751 | 1,190 |
| AvgPool | .927 | .874 | .900 | 294 |
| ReLU | .868 | .859 | .863 | 11,425 |
| ELU | .861 | .945 | .901 | 8,311 |
| LeakyReLU | .962 | .801 | .874 | 3,338 |
| Sigmoid | .462 | .801 | .585 | 5,106 |
| Tanh | .928 | .384 | .543 | 8,050 |
| Weigted Avg. | **.945** | **.945** | **.945** | - |

GTX-1080

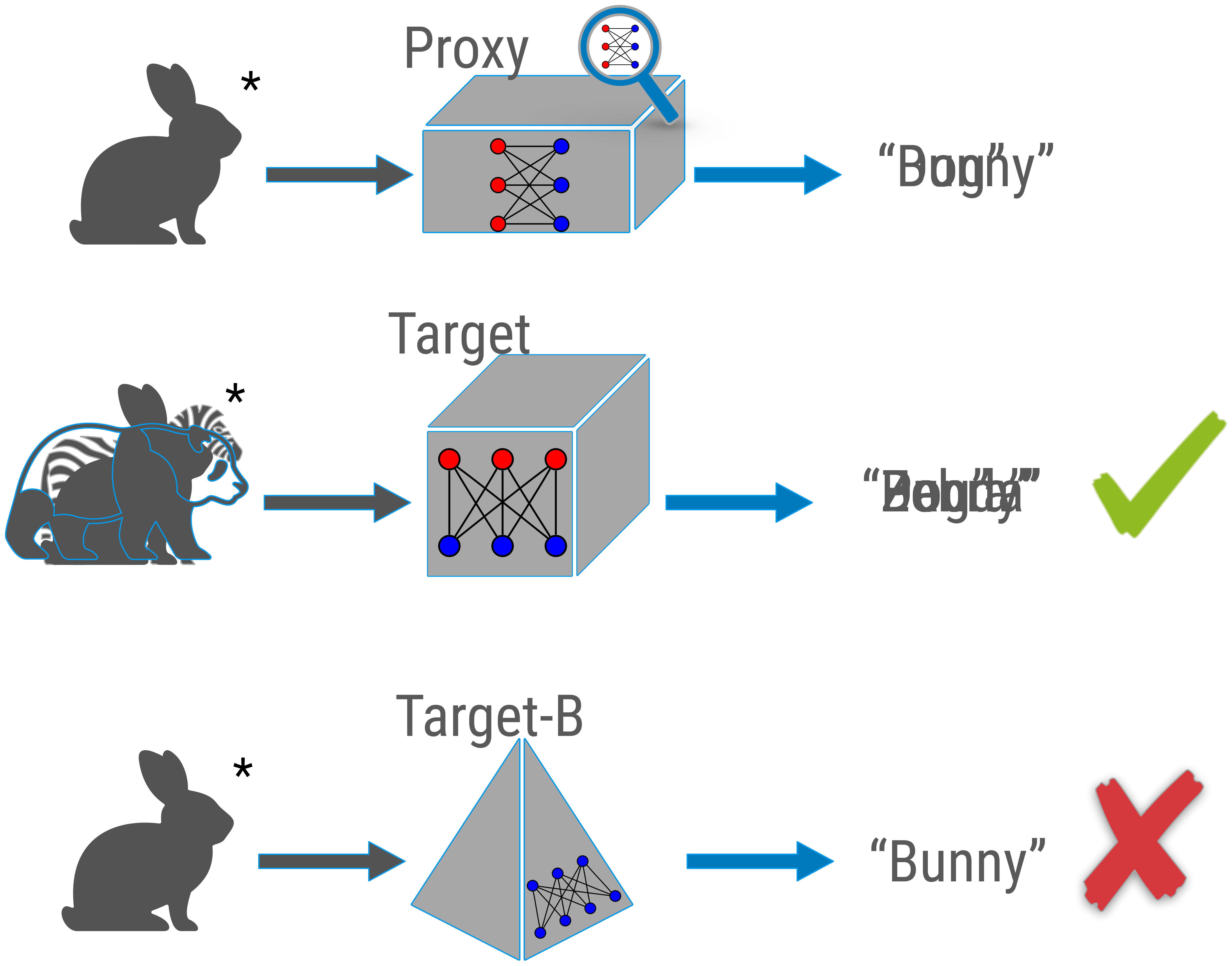


# GPU Transferability

| | Target GPU | | | | | |
|---|---|---|---|---|---|---|
| | GTX-960 | MSI-1060 | MSI-1070 | MSI-1080 | EVGA-1080 | GTX-1080 |
| With Holdout | 61.3 | 77.4 | 83.4 | 87.1 | 93.2 | 93.9 |
| Full Dataset | 96.5 | 88.6 | 93.4 | 91.7 | 95.8 | 95.2 |



# Transfer Attacks

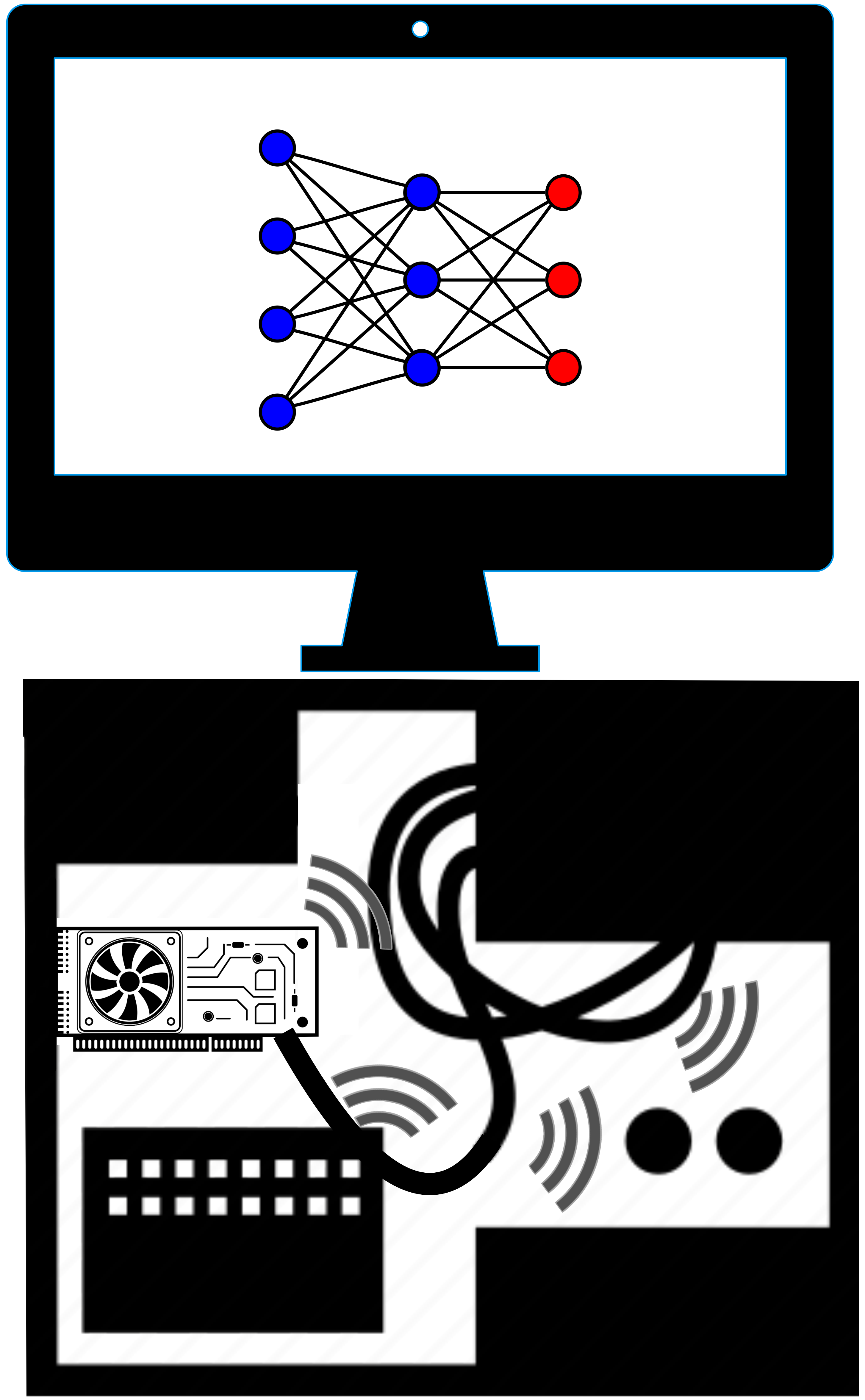


# Transfer Attacks

Target Model

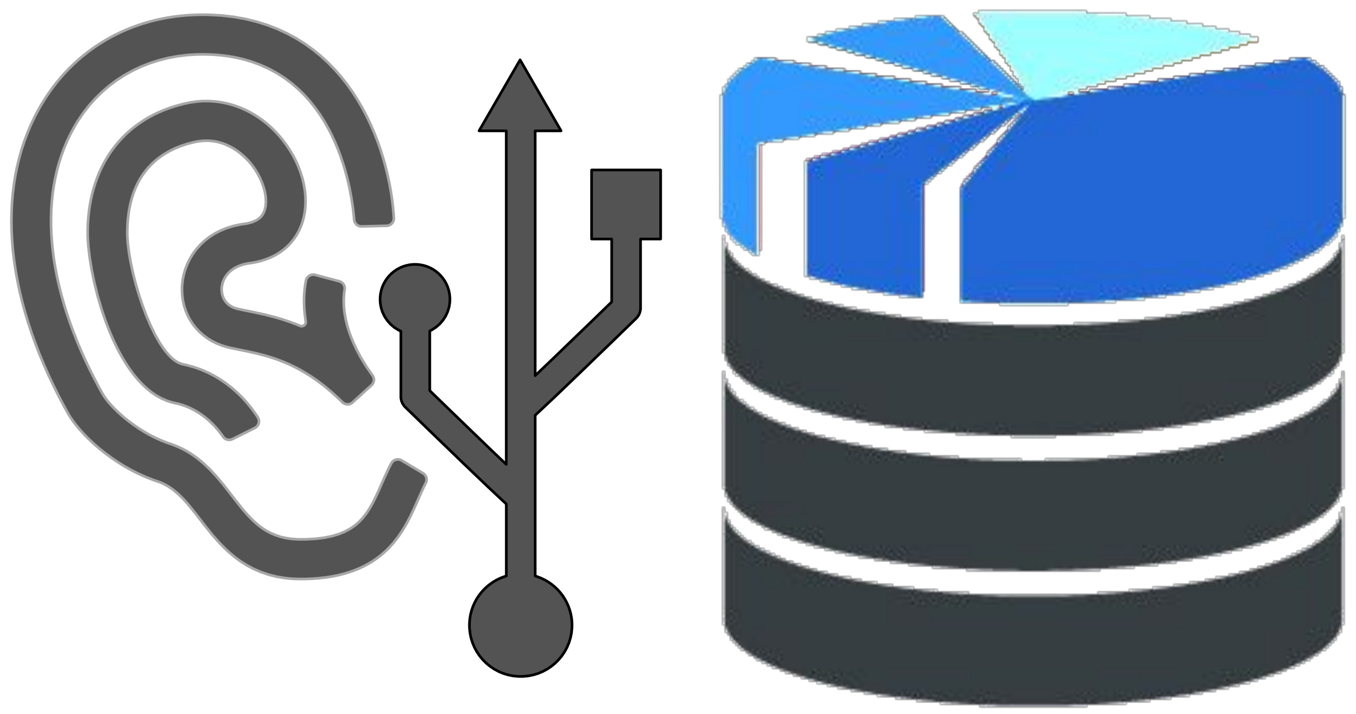
| Proxy Model | ResNet-18 | ResNet-34 | ResNet-101 | VGG-11 | VGG-16 | AlexNet |
|---|---|---|---|---|---|---|
| ResNet-18 | 97.70 | 90.72 | 80.27 | 47.98 | 86.64 | 30.56 |
| ResNet-34 | 97.21 | 92.46 | 82.30 | 51.42 | 85.60 | 32.34 |
| ResNet-101 | 92.53 | 86.98 | 92.95 | 53.98 | 83.04 | 30.55 |
| VGG-11 | 65.86 | 57.82 | 57.52 | 60.24 | 65.50 | 39.95 |
| VGG-16 | 74.00 | 61.54 | 54.23 | 41.60 | 74.29 | 29.57 |
| AlexNet | 10.11 | 9.59 | 10.19 | 11.60 | 10.42 | 62.70 |

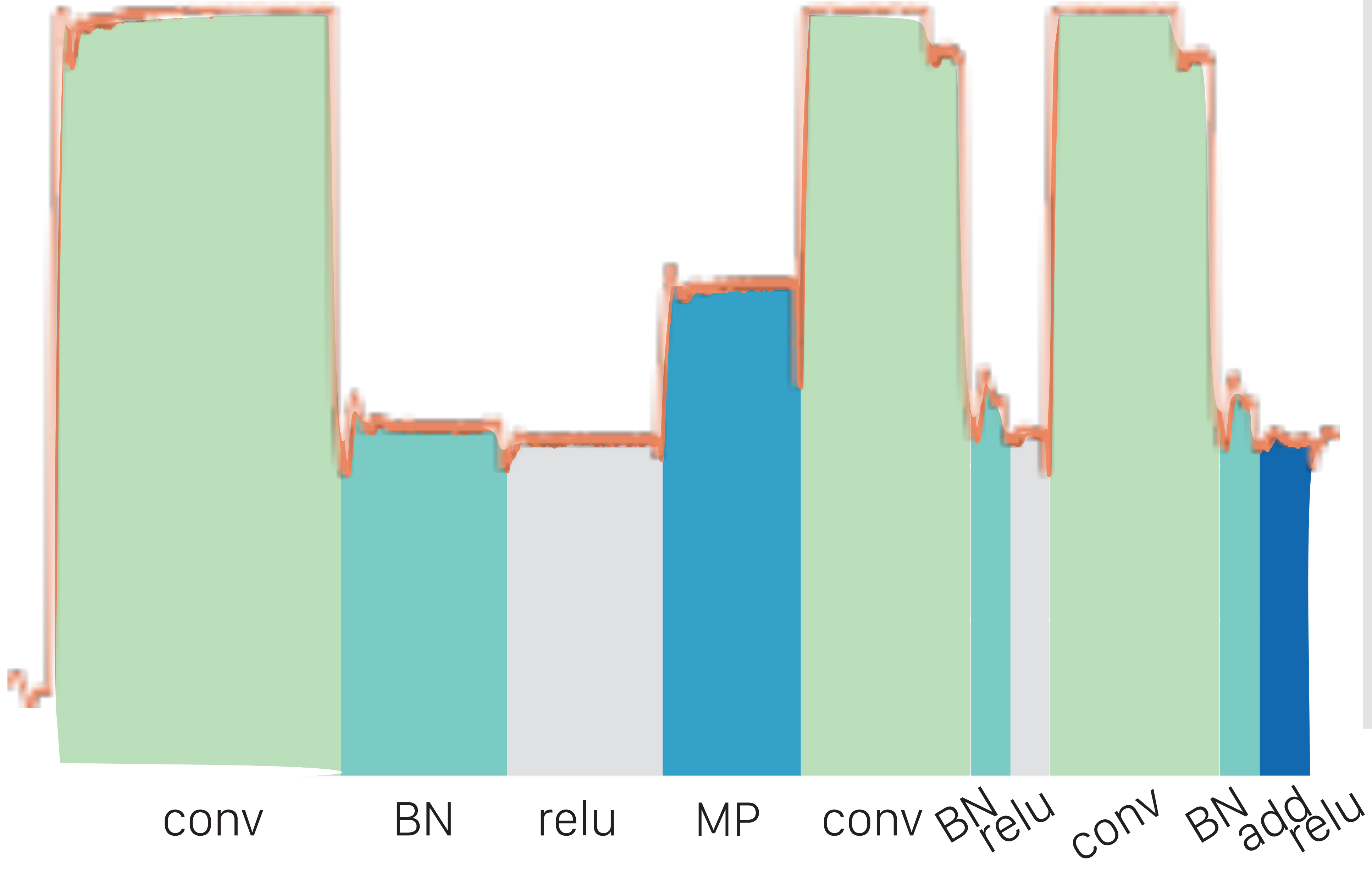
# Applying our Methodology



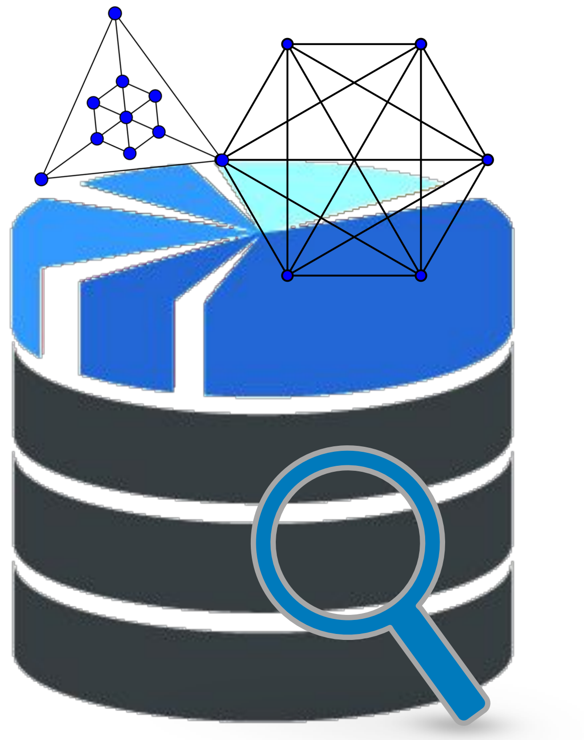
Methodology

- ➡Generate large signal dataset
- ➡Identify network invariant behavior
- ➡Distill layer sequences into graphs
- ➡Optimize estimates to extract model



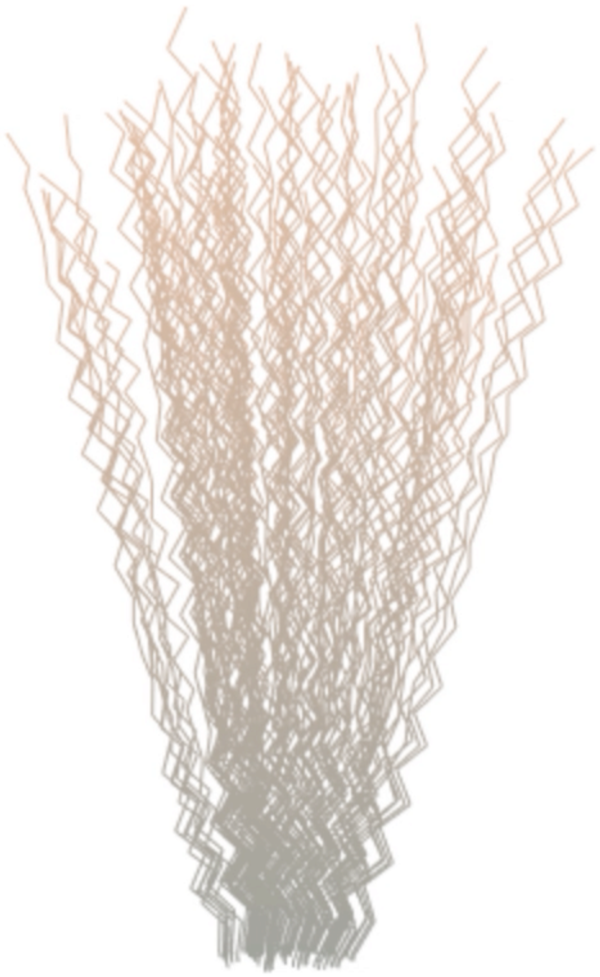


# Roadmap



Additive
Manufacturing

Side-channel
Security



Physics-based
Contact

# Data-Driven Hair Contact:

## Resolving Collisions with GraphNets

with Eitan Grinspun, Changxi Zheng

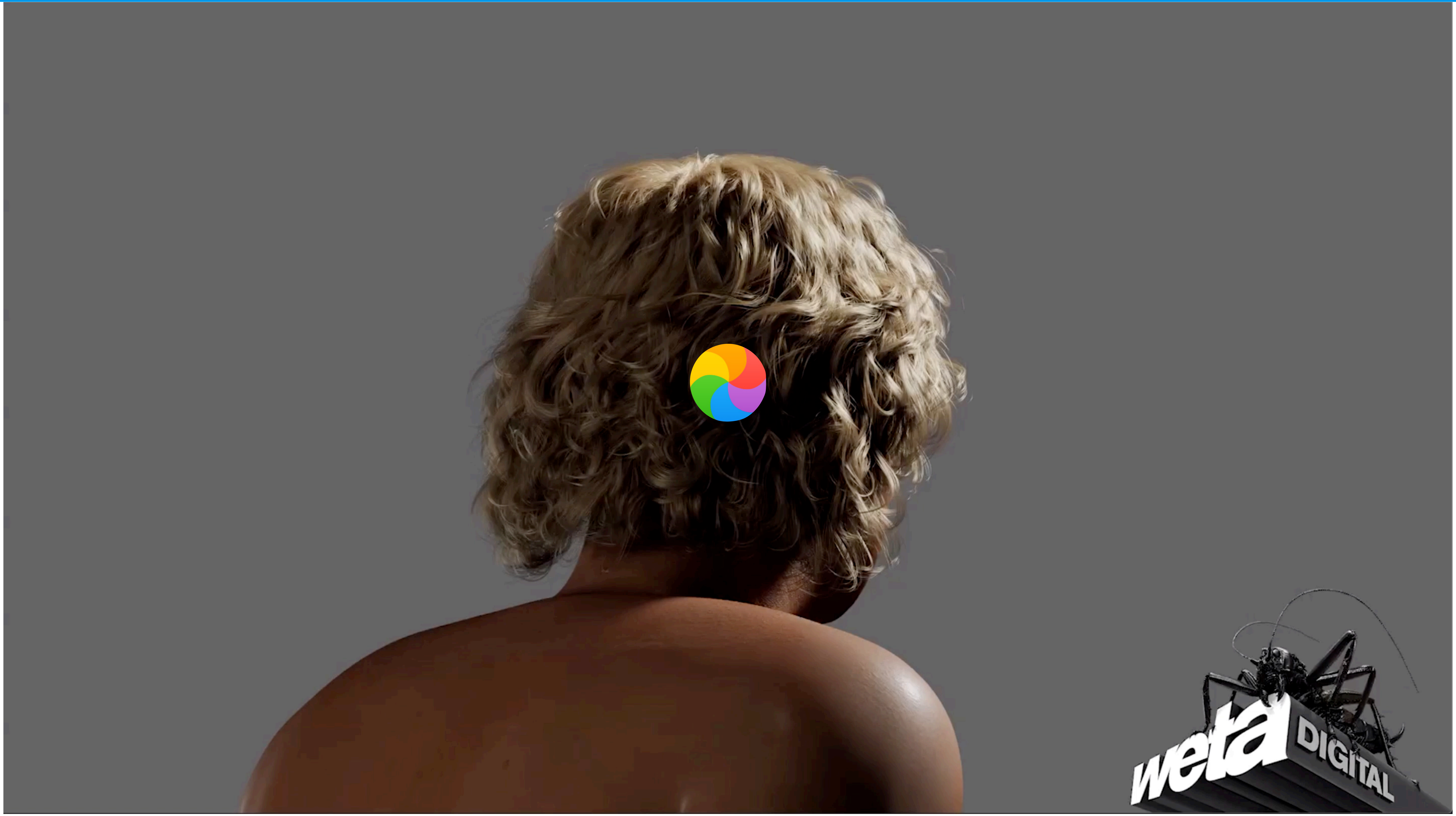
COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

UNIVERSITY OF TORONTO



[Ongoing research]

# Hair Simulation



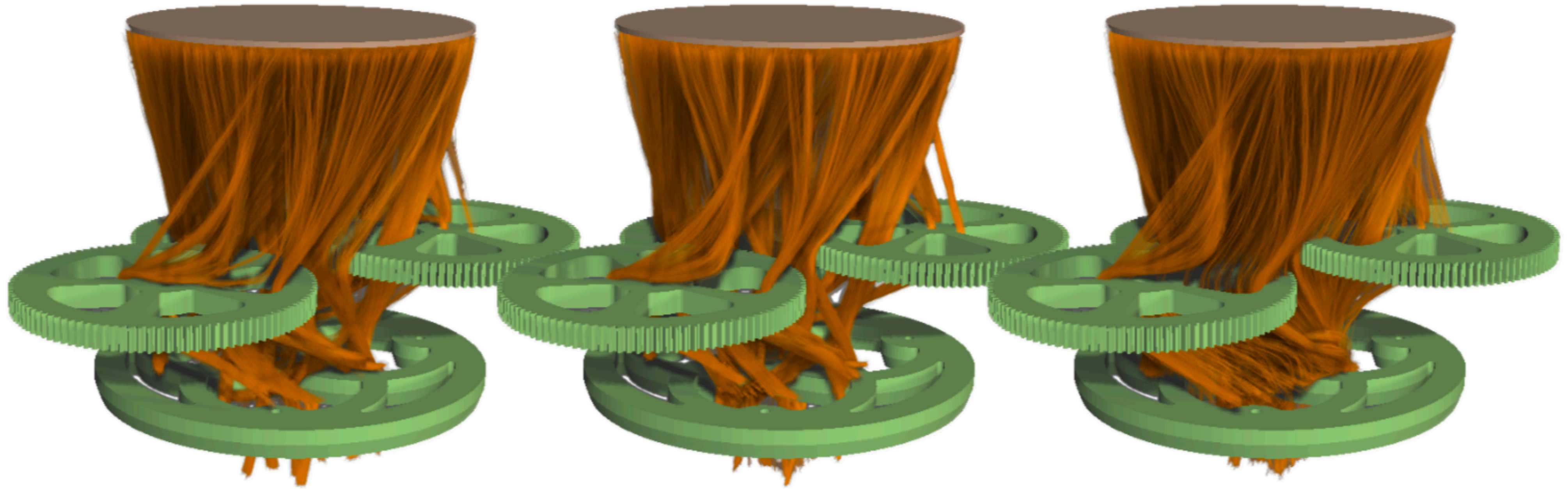
# Towards Faster Hair

Hair-Meshes

Rod-Skinning

Non-linear Elasticity

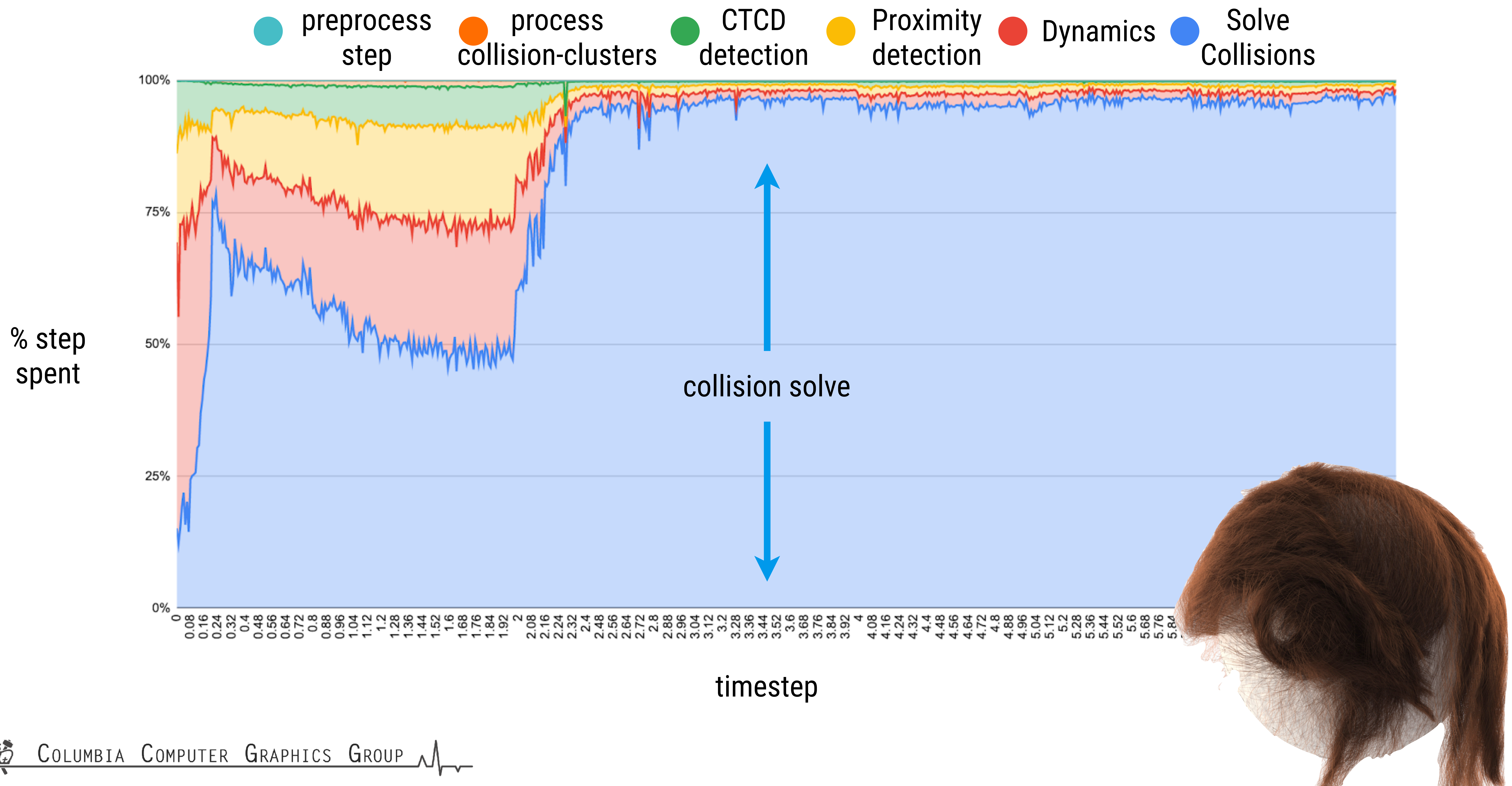
Real-Time Hair Mesh Simulation
[Wu & Yuksel 2016]



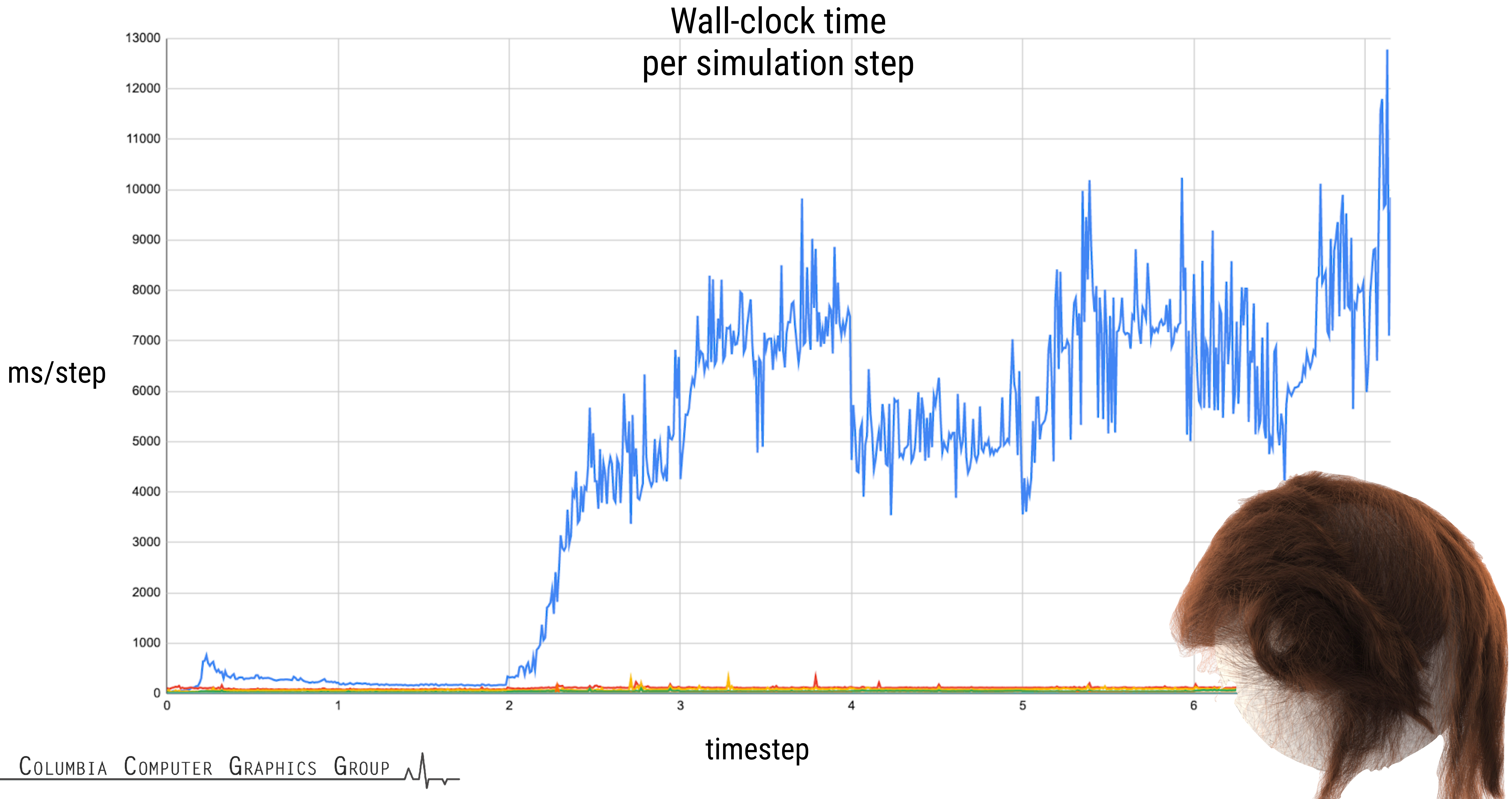
Adaptive Skinning for Interactive
Hair-Solid Simulation
[Chai et al. 2016]

Adaptive Nonlinearity for Collisions in
Complex Rod Assemblies
[Kaufman et al. 2014]

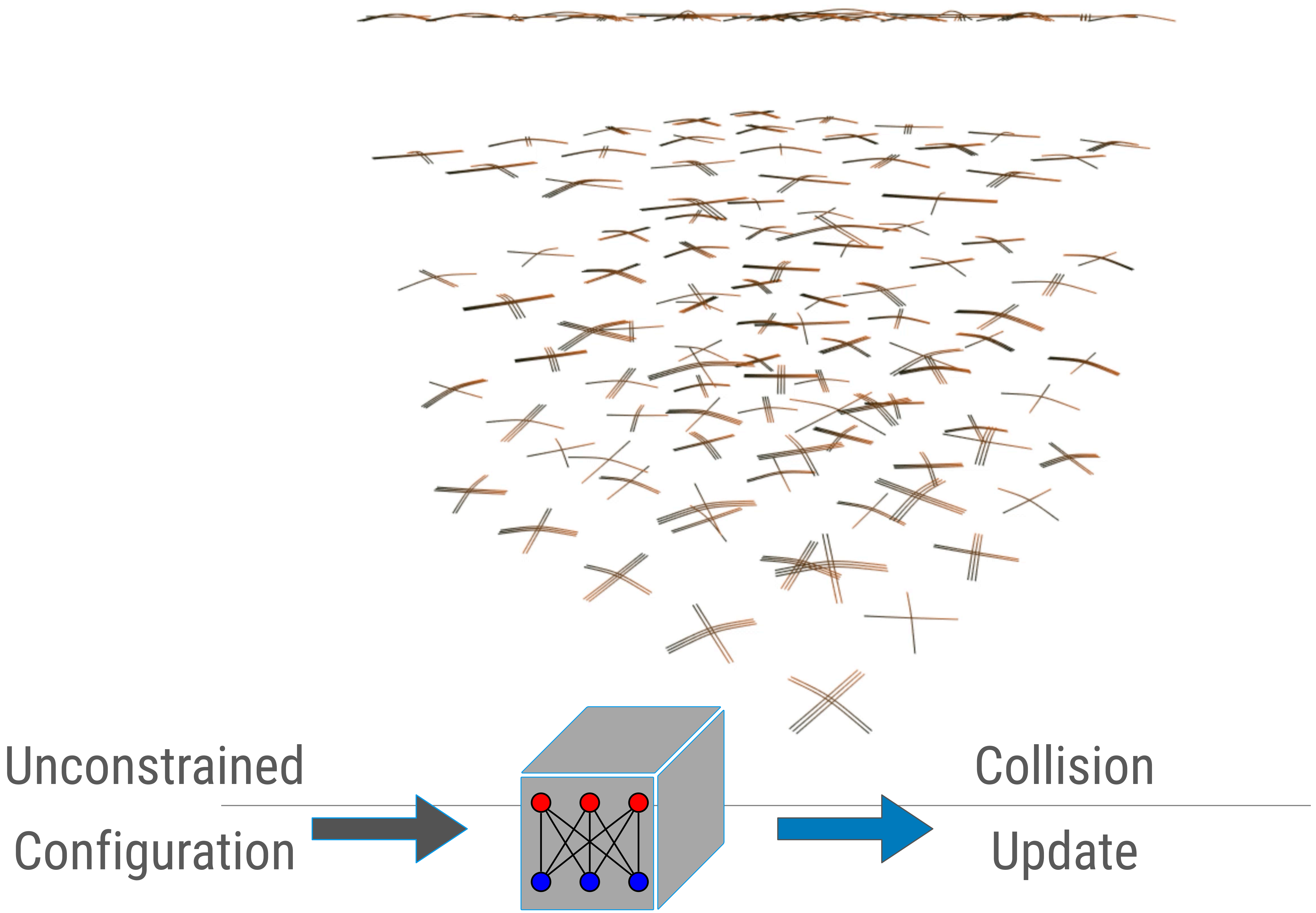
# Bottleneck - step breakdown



# Bottleneck - absolute time



# Data Abundance



# Objective

speed

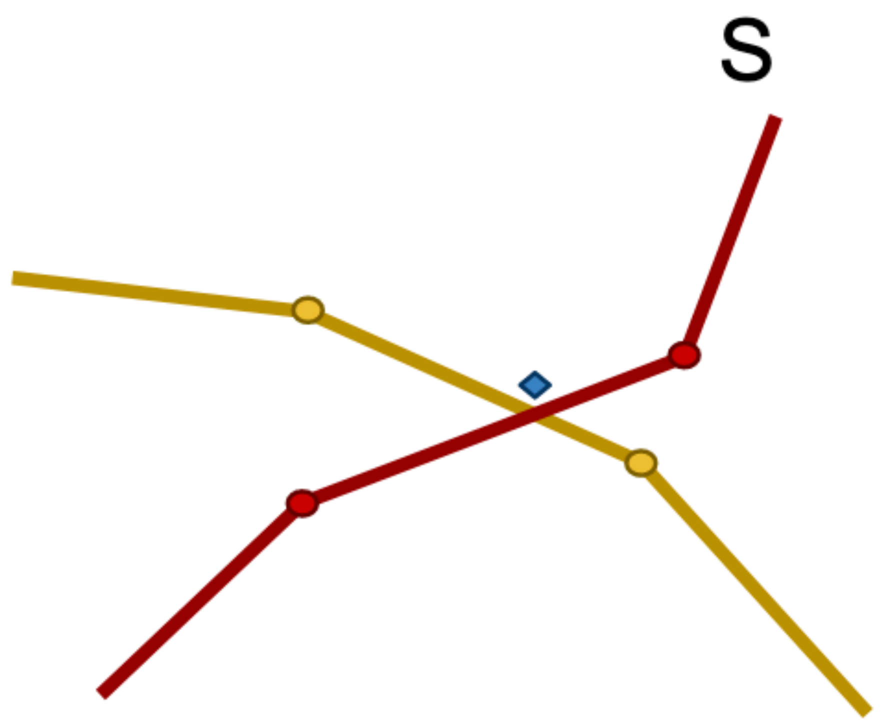
visual quality

**_Approximations are okay!_**

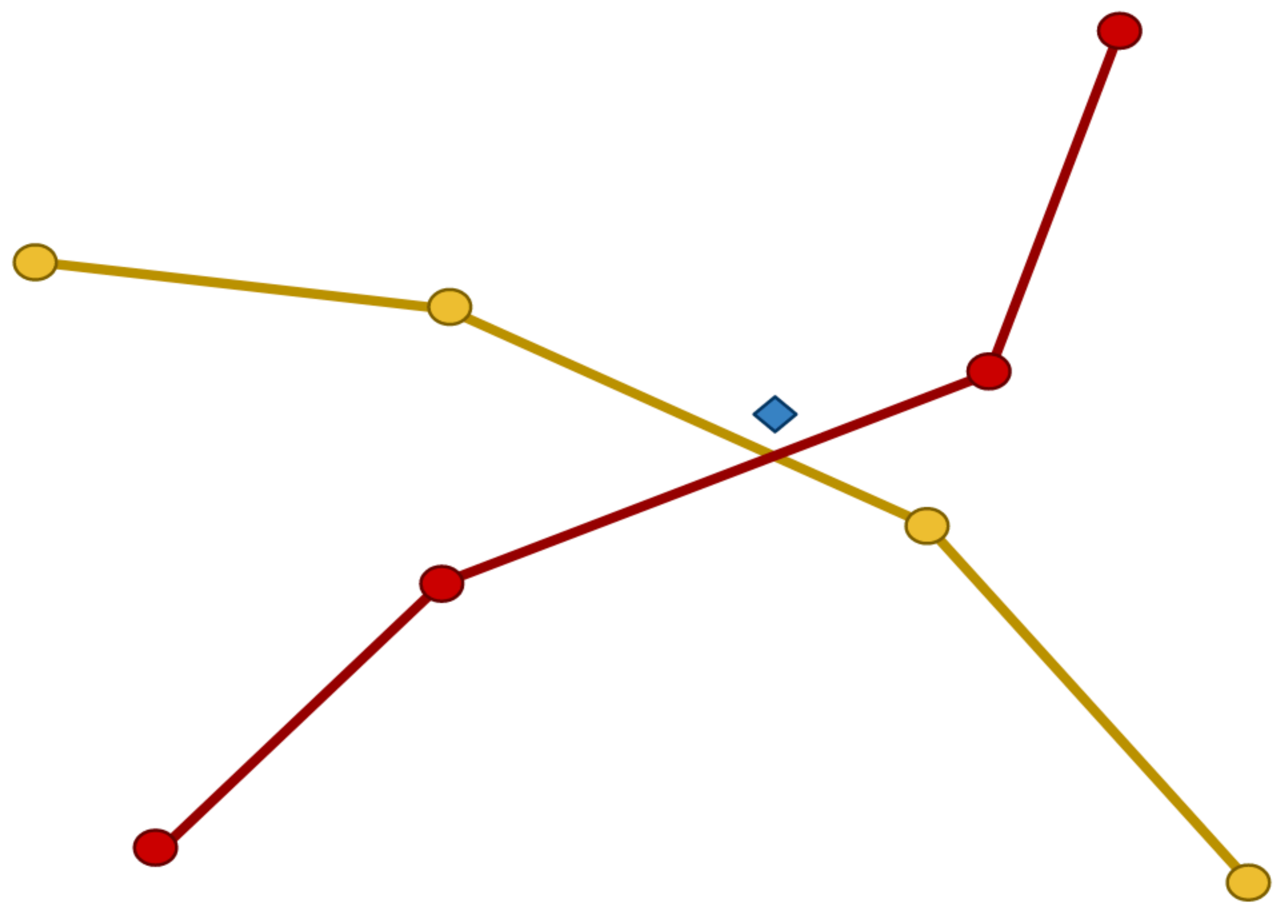
robustness

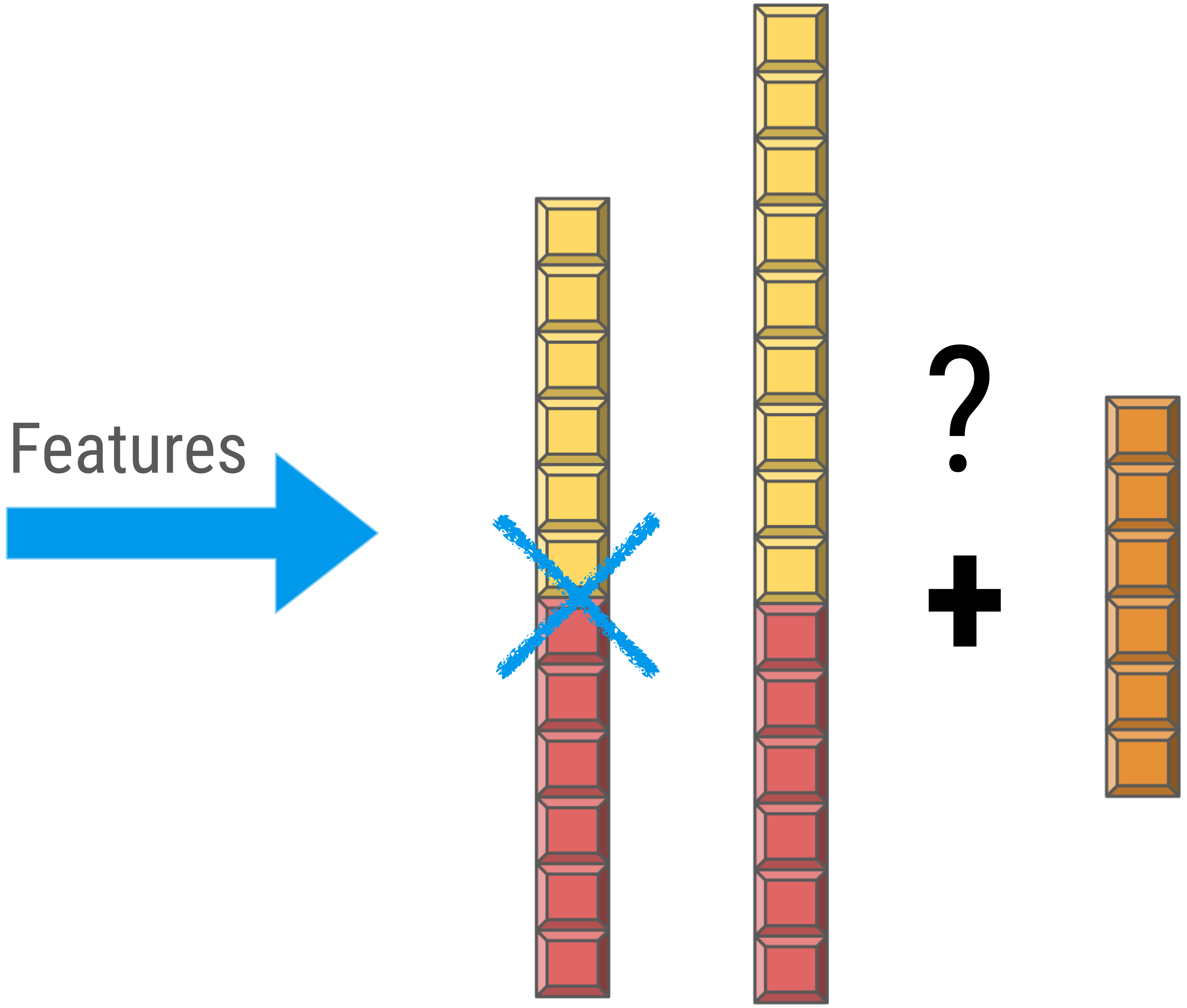
flexibility

# Shaping the Inputs



# Shaping the Inputs





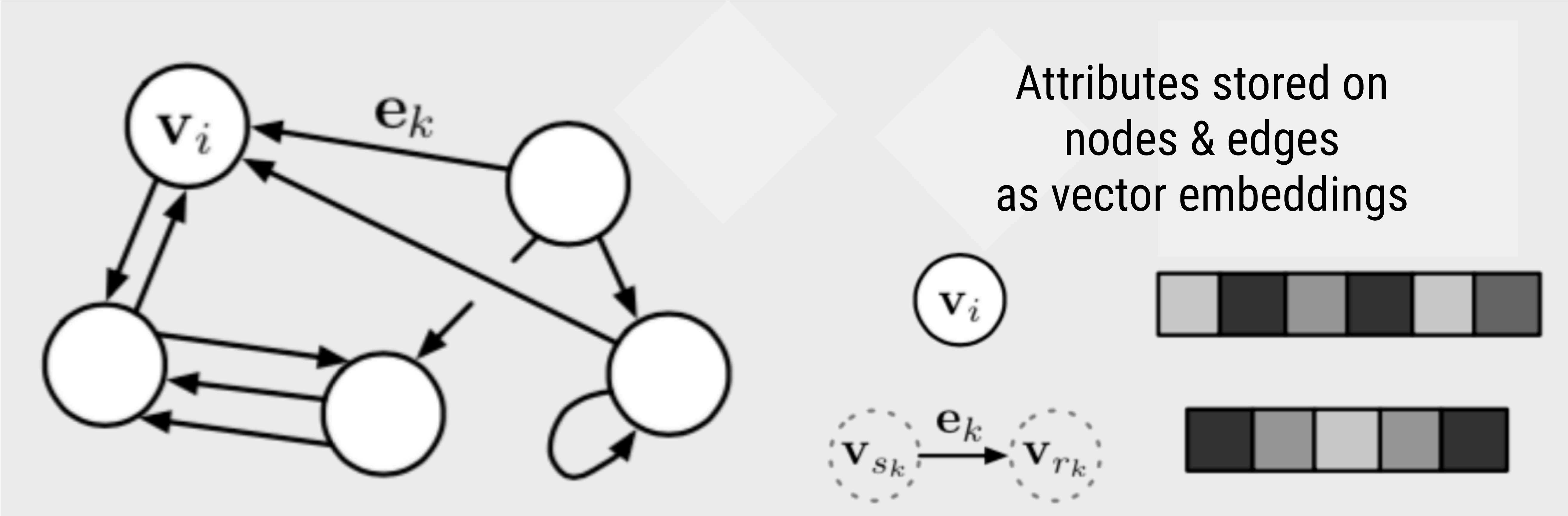
# GraphNets

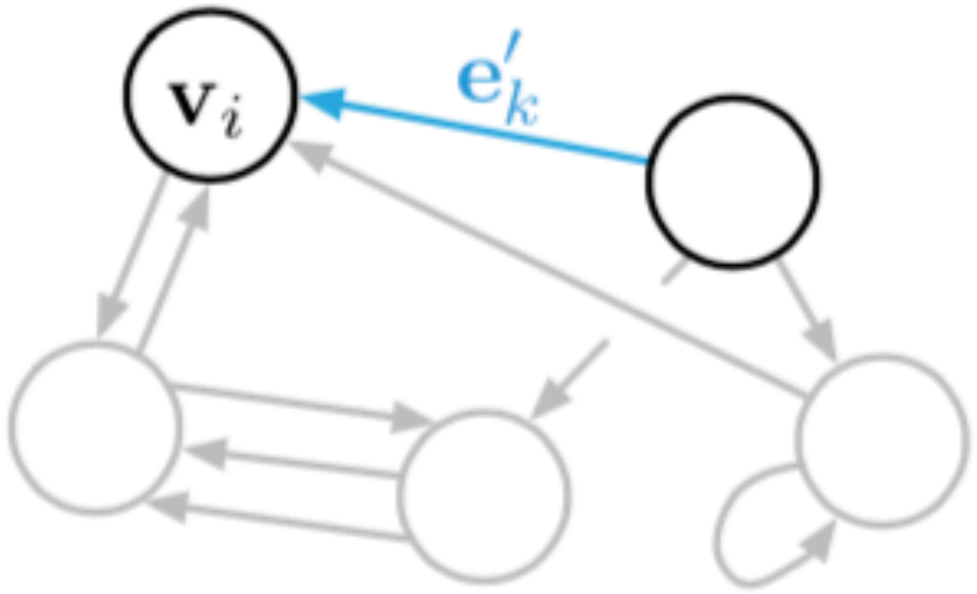
**Algorithm 1** Steps of computation in a full GN block.

**function** GraphNetwork($E$, $V$, $\mathbf{u}$)
  **for** $k \in \{1 \ldots N^e\}$ **do**
    $\mathbf{e}'_k \leftarrow \phi^e\left(\mathbf{e}_k, \mathbf{v}_{r_k}, \mathbf{v}_{s_k}, \mathbf{u}\right)$
  **end for**
  **for** $i \in \{1 \ldots N^n\}$ **do**
    **let** $E'_i = \{(\mathbf{e}'_k, r_k, s_k)\}_{r_k=i,\ k=1:N^e}$
    $\bar{\mathbf{e}}'_i \leftarrow \rho^{e \rightarrow v}\left(E'_i\right)$
    $\mathbf{v}'_i \leftarrow \phi^v\left(\bar{\mathbf{e}}'_i, \mathbf{v}_i, \mathbf{u}\right)$
  **end for**
  **let** $V' = \{\mathbf{v}'\}_{i=1:N^v}$
  **let** $E' = \{(\mathbf{e}'_k, r_k, s_k)\}_{k=1:N^e}$
  $\bar{\mathbf{e}}' \leftarrow \rho^{e \rightarrow u}\left(E'\right)$
  $\bar{\mathbf{v}}' \leftarrow \rho^{v \rightarrow u}\left(V'\right)$
  $\mathbf{u}' \leftarrow \phi^u\left(\bar{\mathbf{e}}', \bar{\mathbf{v}}', \mathbf{u}\right)$
  **return** $(E', V', \mathbf{u}')$
**end function**

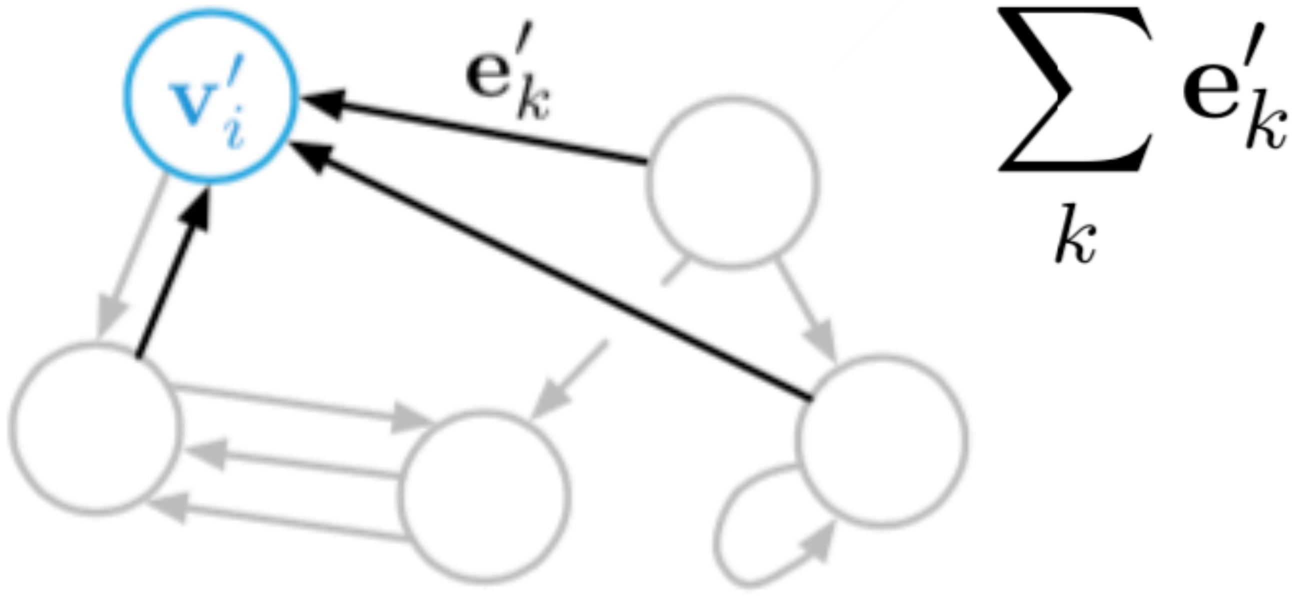
Relational inductive biases, deep learning and graph networks [Battaglia et al. 2018]

Multi-Graph allows for nodes with self-edges and multi-edge connections



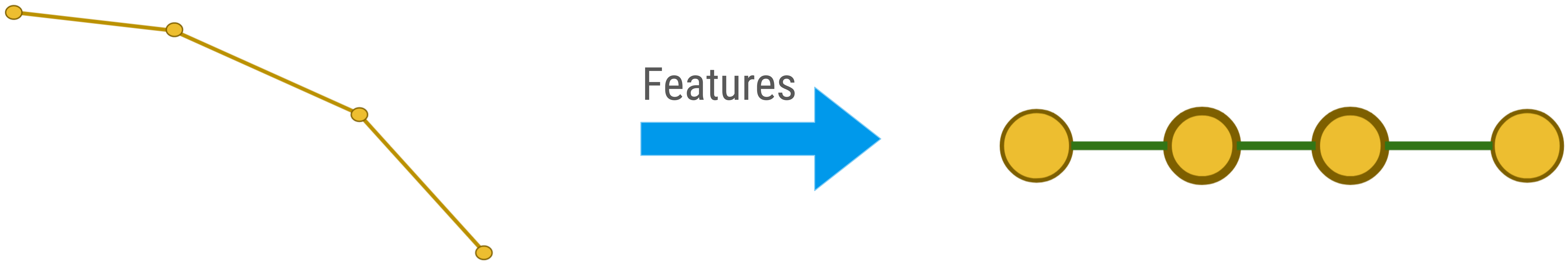




edges update with sender & receiver nodes

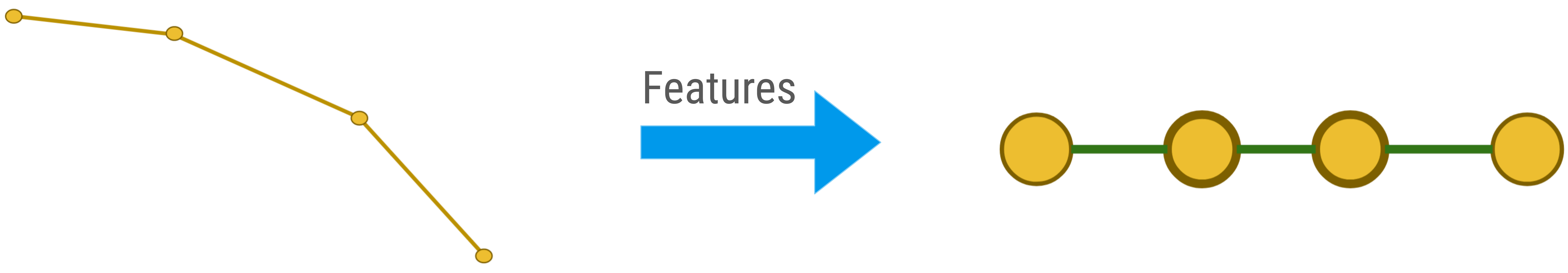



nodes update by aggregating incident edges

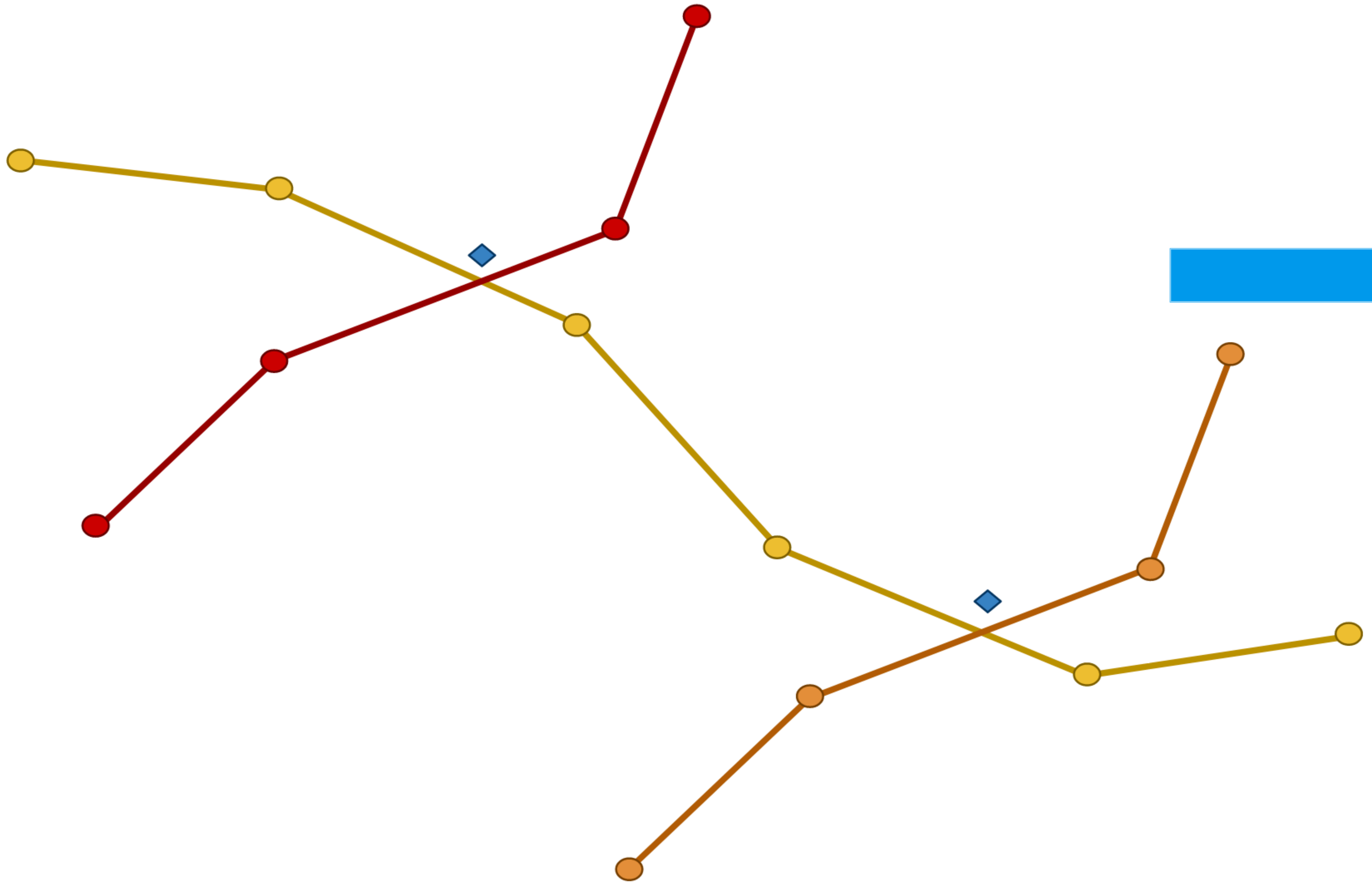
# Strands to Graphs

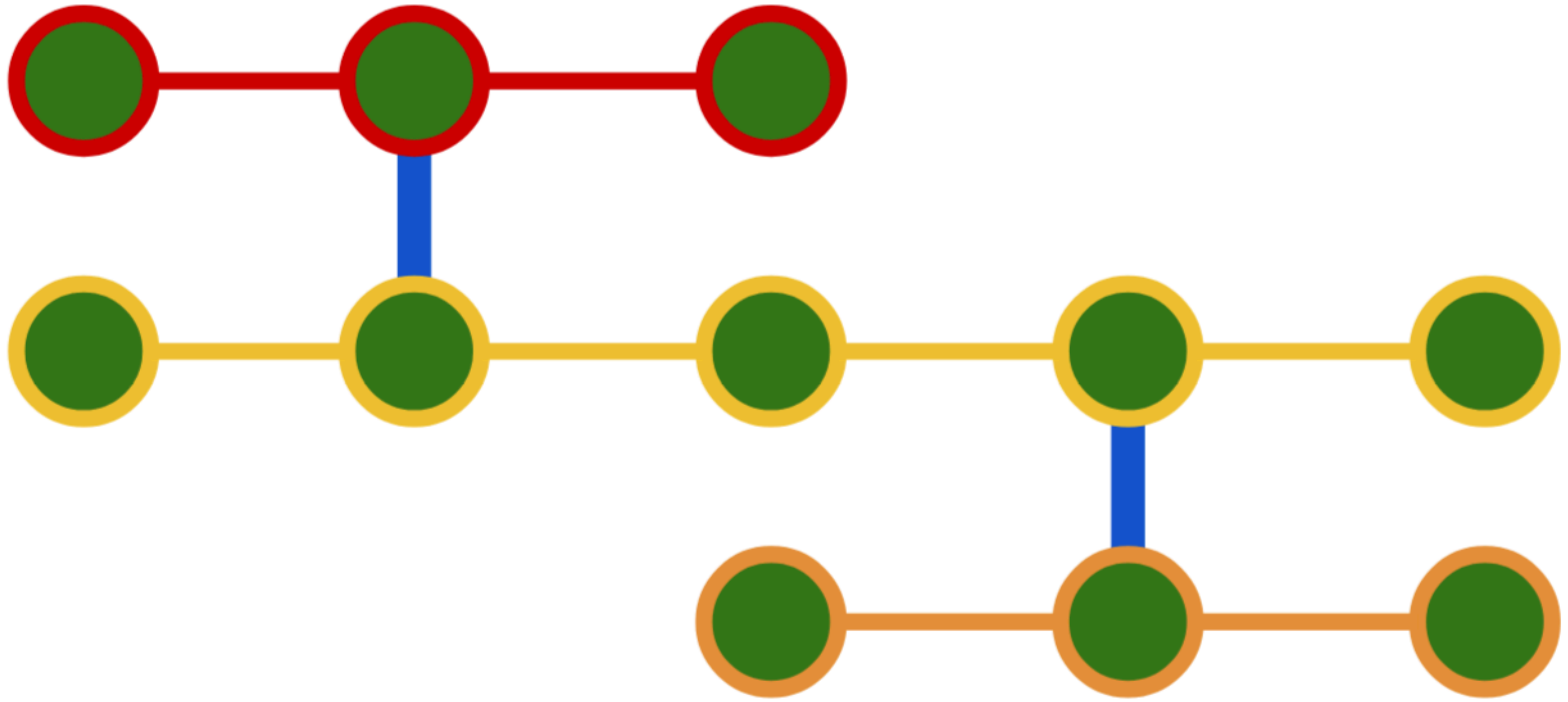


# Strands to Graphs

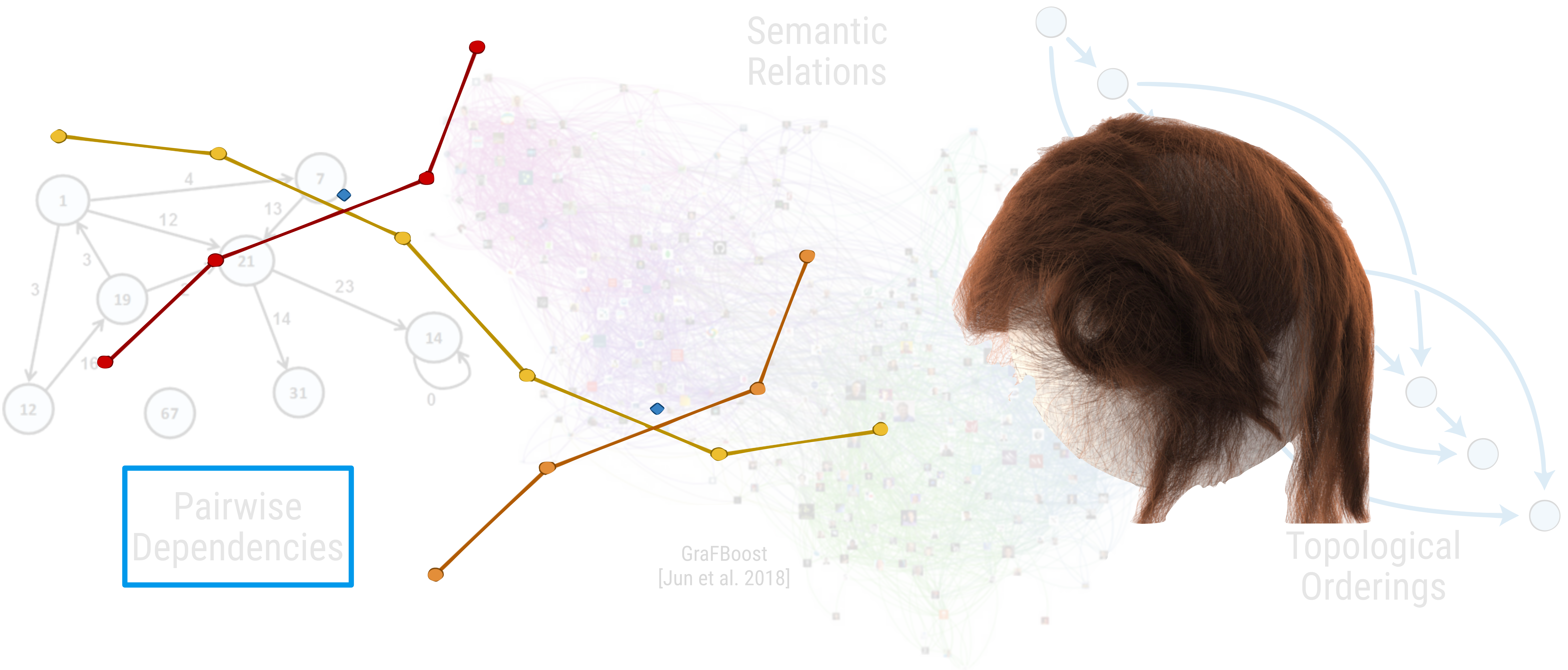


# Strands to Graphs

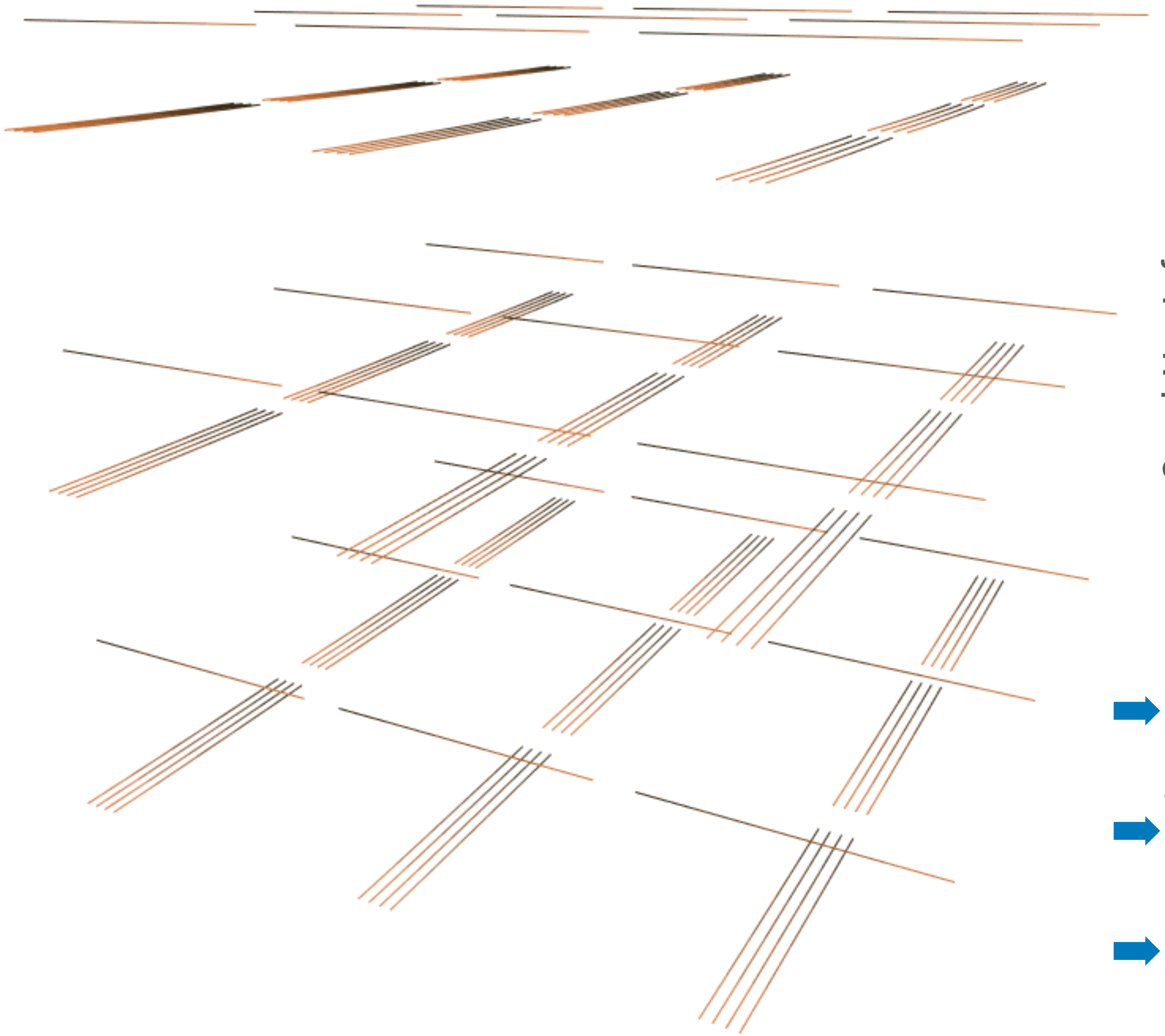




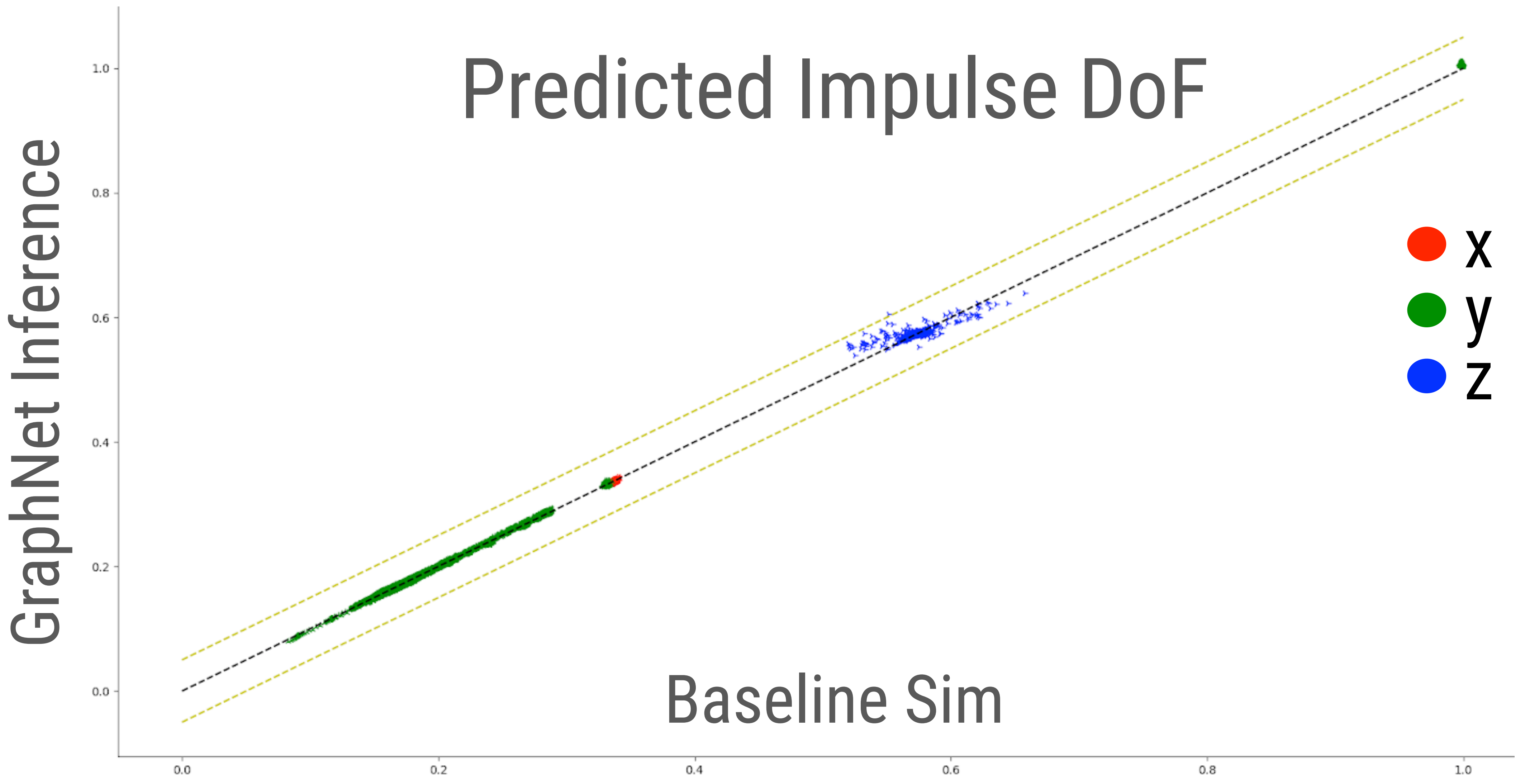
# Contact Dual GraphNets



# Preliminary Results

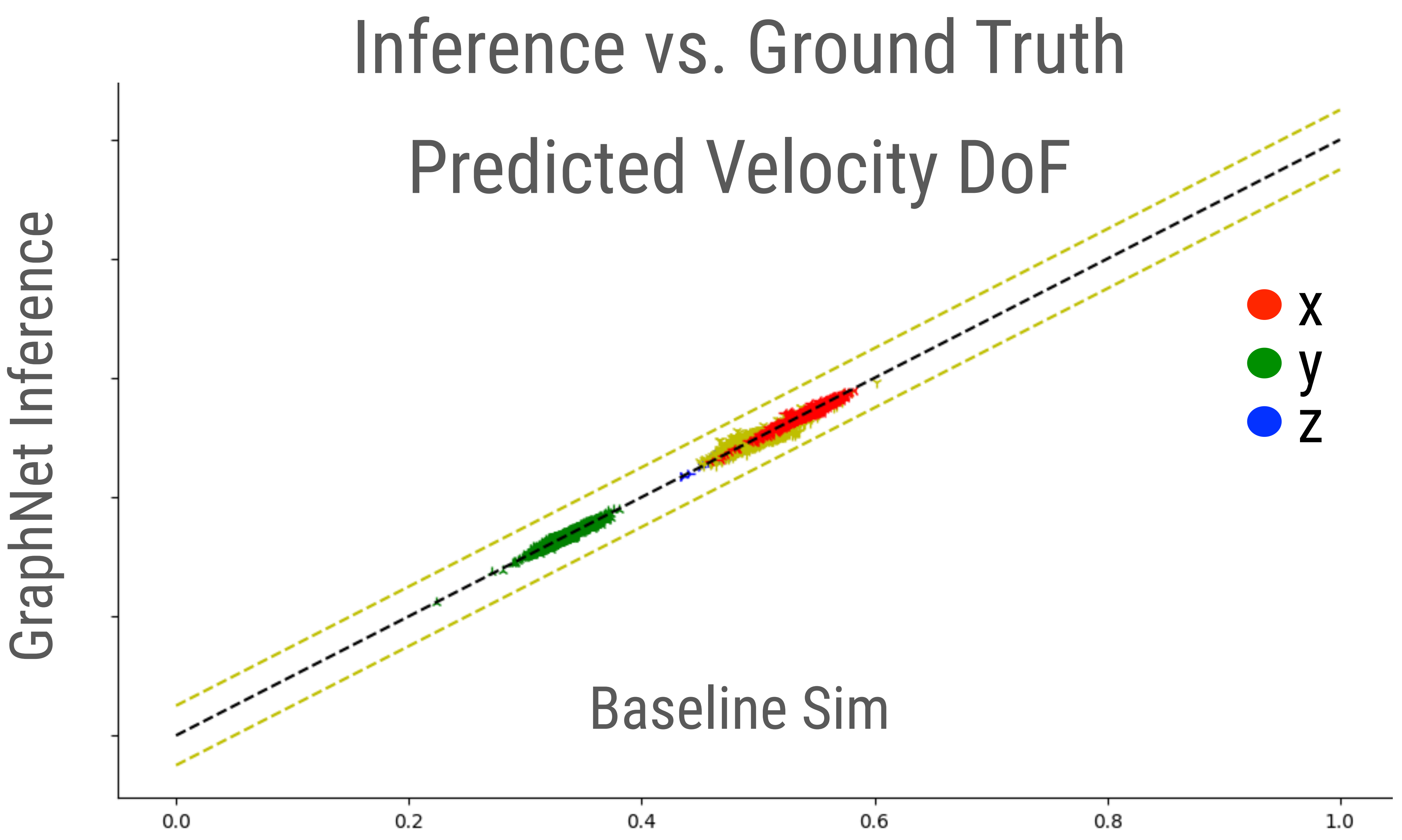


Inference vs. Ground Truth




- Perturbed initial conditions
- Varying DoF / Strand
- Stable resting contact

# Next Steps

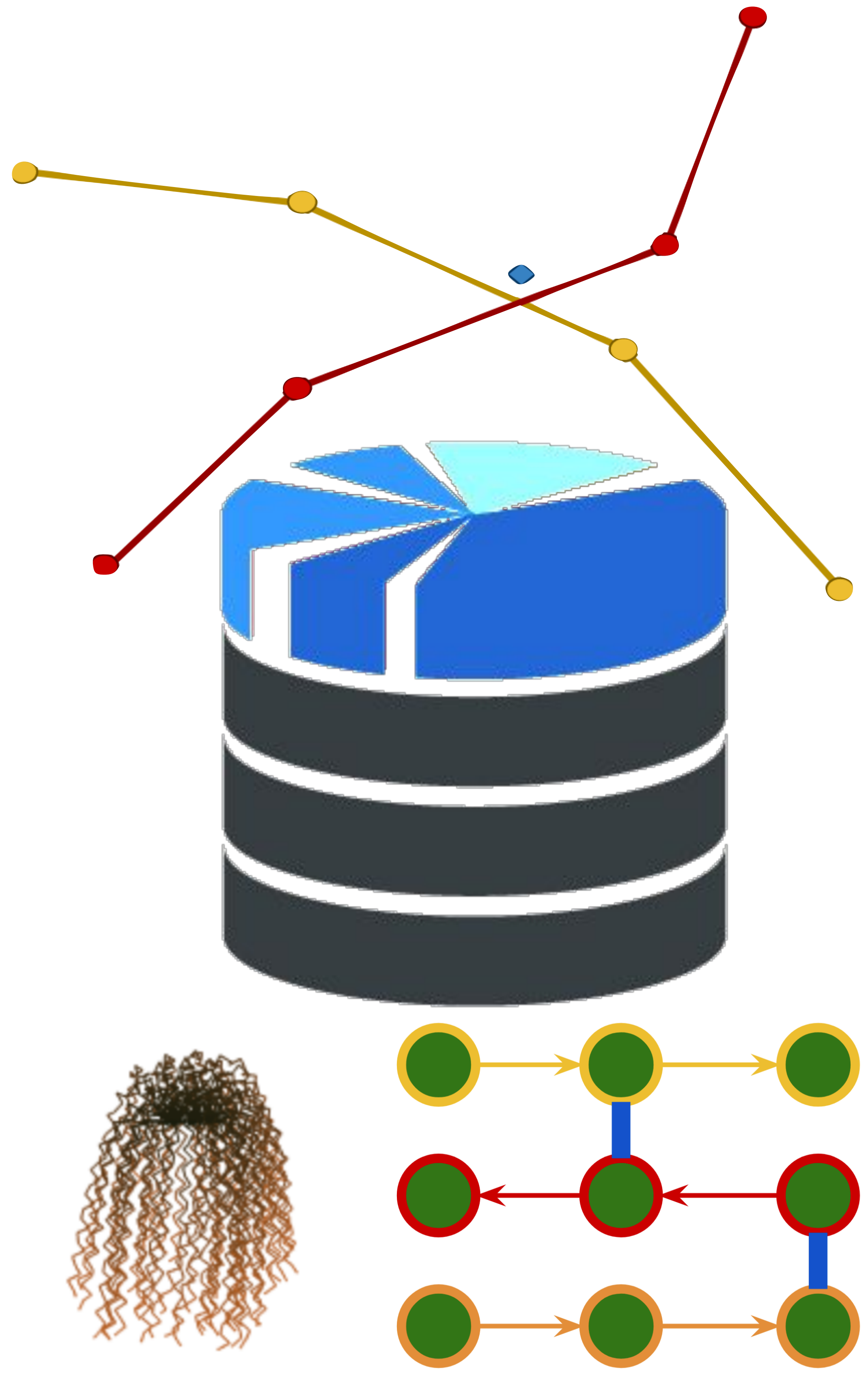



- More complex interactions
- Larger contact graph
- Non-straight hair model

# Overview

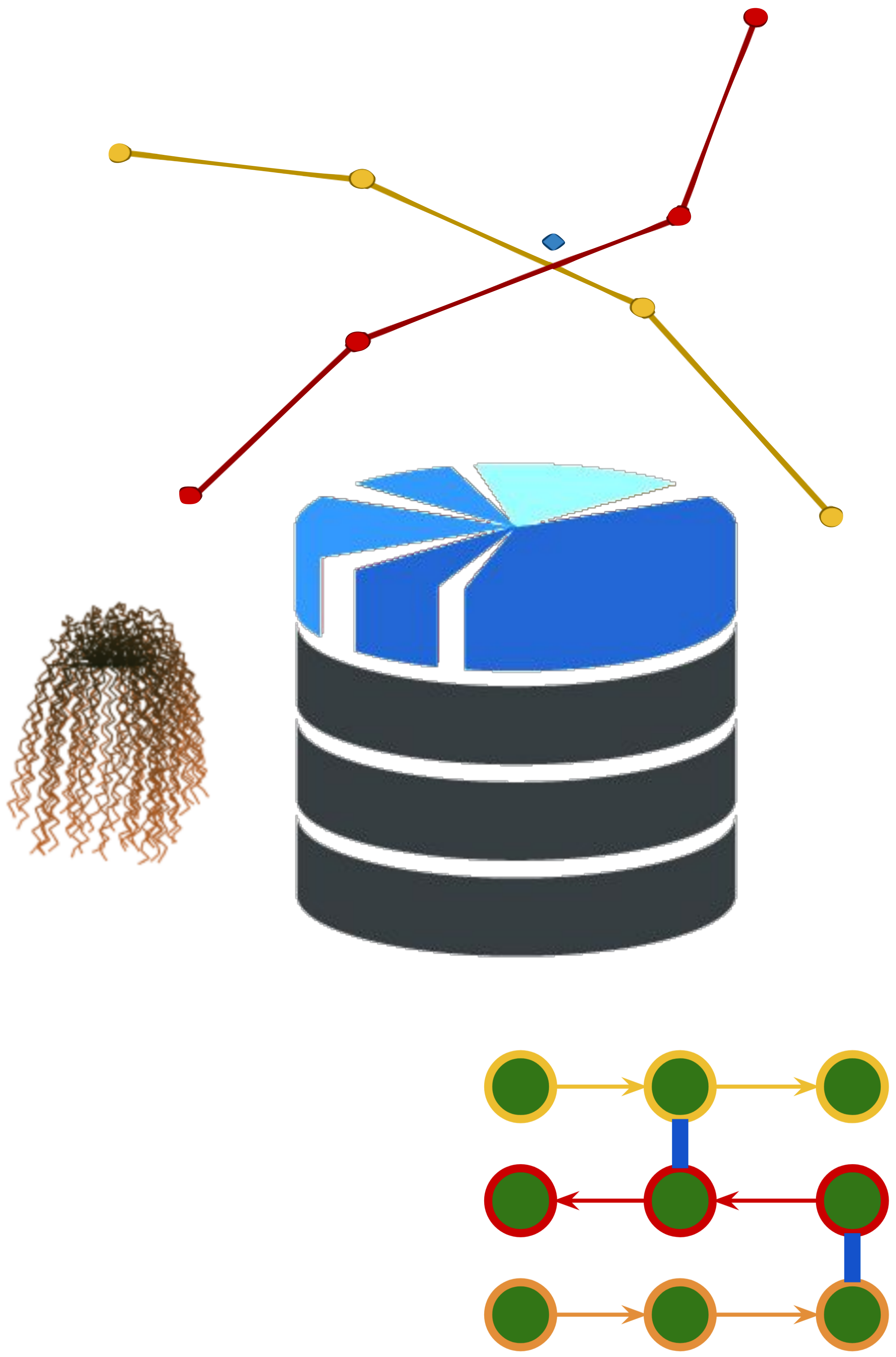
## Fits the Methodology:

- ➡Generate large contact dataset
- ➡Identify contact features
- ➡Map strands & collisions into graphs
- ➡Train fast feed-forward contact-graphs



# Contributions

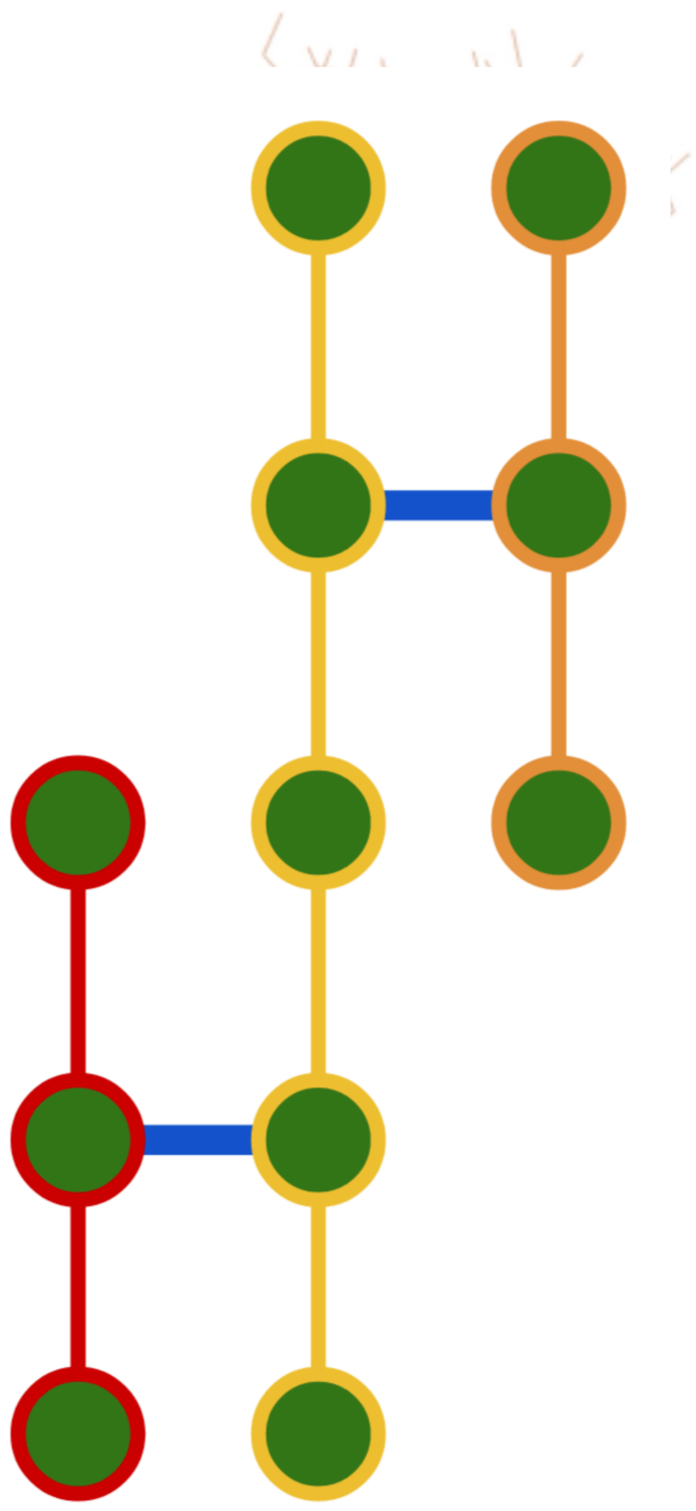
- Fast
- Stable
- Flexible
- Model agnostic
- Paves the way for future hair & ML
  - a novel GraphNet formulation



# Return to Roadmap

LayerCodes

Neural Snooping



Data-Driven Hair Contact

# Timeline

- ✓ LayerCodes - Fall 2019
- ✓ Neural Snooping - Fall 2021
- ❖ Thesis Proposal - Winter 2021/2022
- ❖ Data-Driven Hair Contact Submission - Spring 2022
- ❖ Thesis Writing - Spring 2022
- ❖ Thesis Defense - Summer 2022

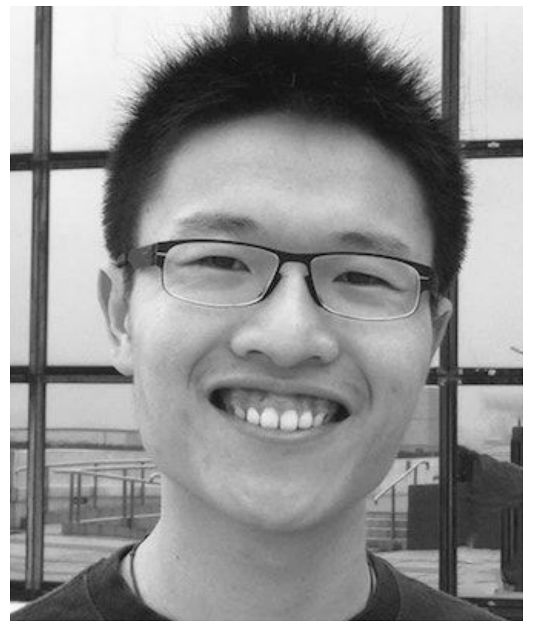
# Acknowledgments

advisors

Eitan Grinspun

Changxi Zheng

co-authors



Dingzeyu Li

Yuan Yang

Chang Xiao

Raymond Fei

- Oded Stein
- Peter Chen
- Joni Mici
- Mohammed Haroun
- William Miller
- Qingnan Zhou
- Anne Fleming
- Hod Lipson
- Christopher Batty
- David Watkins-Valls
- Carmine Elvezio

PyTorch

NSF

IBM CPLEX

GEM
THE NATIONAL GEM CONSORTIUM

libigl

Thingi10K

COLUMBIA COMPUTER GRAPHICS GROUP

# Questions?

henrique@cs.columbia.edu