Time-aware Robustness of Temporal Graph Neural Networks

Marco Sälzer Silvia Beddar-Wiesing

University of Kassel, Germany

Robustness in the Context of Neural Networks

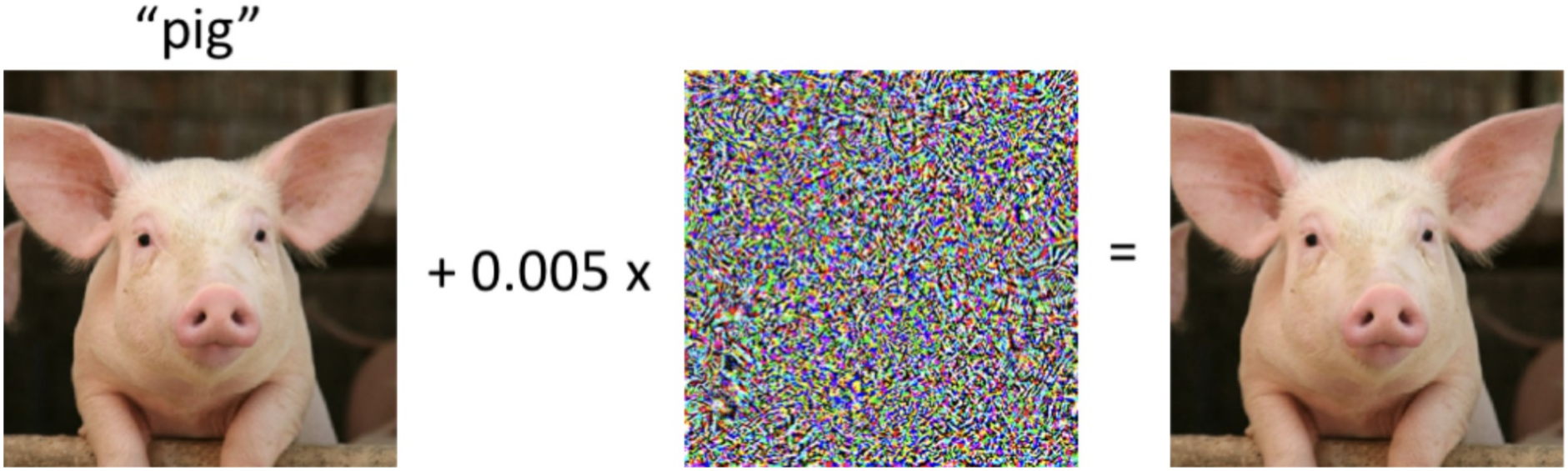
Madry & Schmidt, 2018

Robustness in the Context of Neural Networks

"pig"

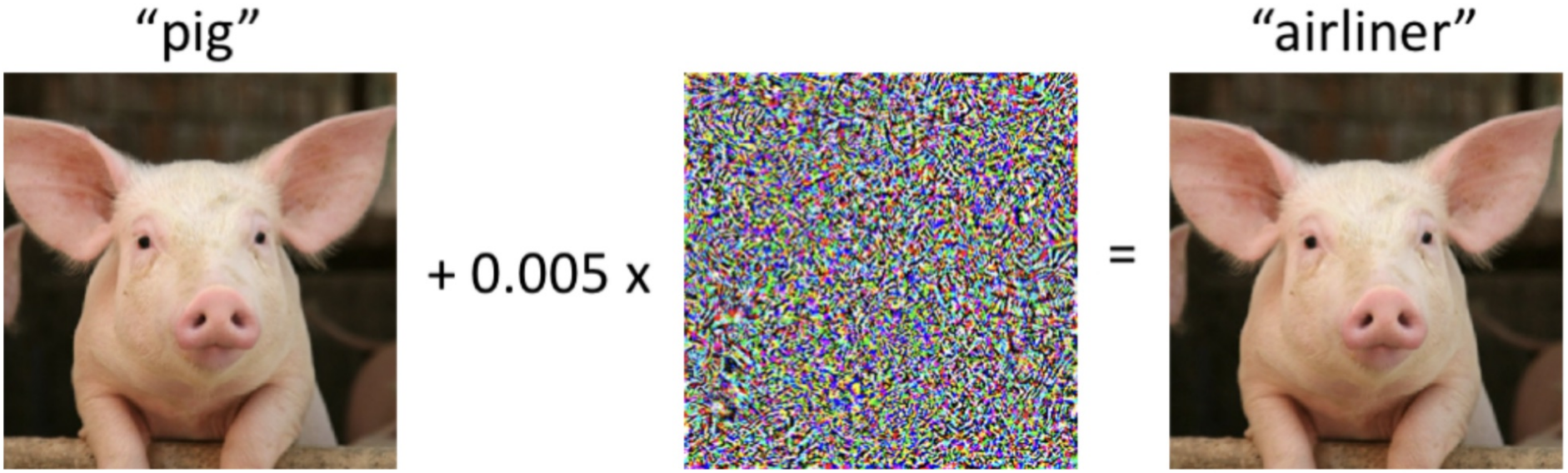
Madry & Schmidt, 2018

Robustness in the Context of Neural Networks



Madry & Schmidt, 2018

Robustness in the Context of Neural Networks



Madry & Schmidt, 2018

Pointwise - Robustness over Real-Valued Data

We call $P = (\bar{x}, B)$ a robustness property where

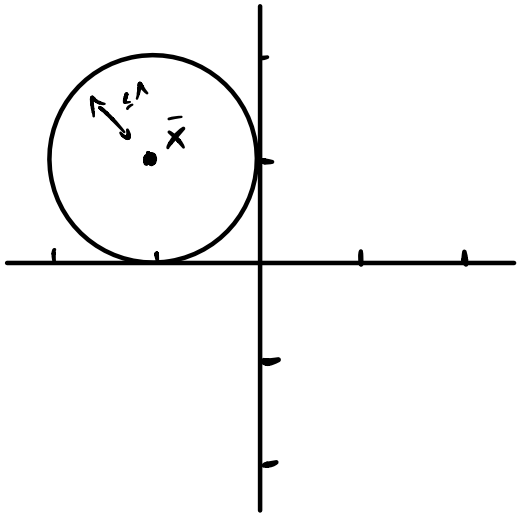
- $\bar{x}$ is some vector, called center-point
- B is some budget of allowed perturbations

Pointwise - Robustness over Real-Valued Data

We call $P = (\bar{x}, B)$ a robustness property where

- $\bar{x}$ is some vector, called center-point
- B is some budget of allowed perturbations

Example: $P = \left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \{ \bar{x}' \mid \| \begin{pmatrix} 1 \\ -1 \end{pmatrix} - \bar{x}' \| \leq 1 \} \right)$

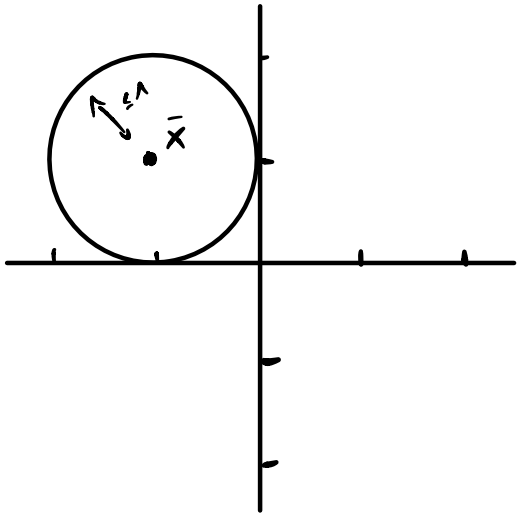


Pointwise - Robustness over Real-Valued Data

We call $P = (\bar{x}, B)$ a robustness property where

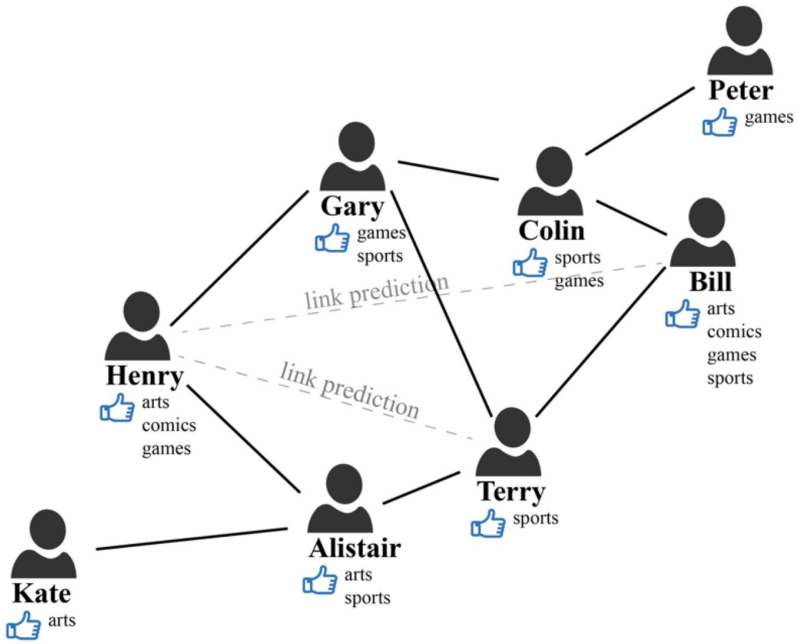
- $\bar{x}$ is some vector, called center-point
- B is some budget of allowed perturbations

Example: $P = \left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \{ \bar{x}' \mid \| \begin{pmatrix} 1 \\ -1 \end{pmatrix} - \bar{x}' \| \leq 1 \} \right)$

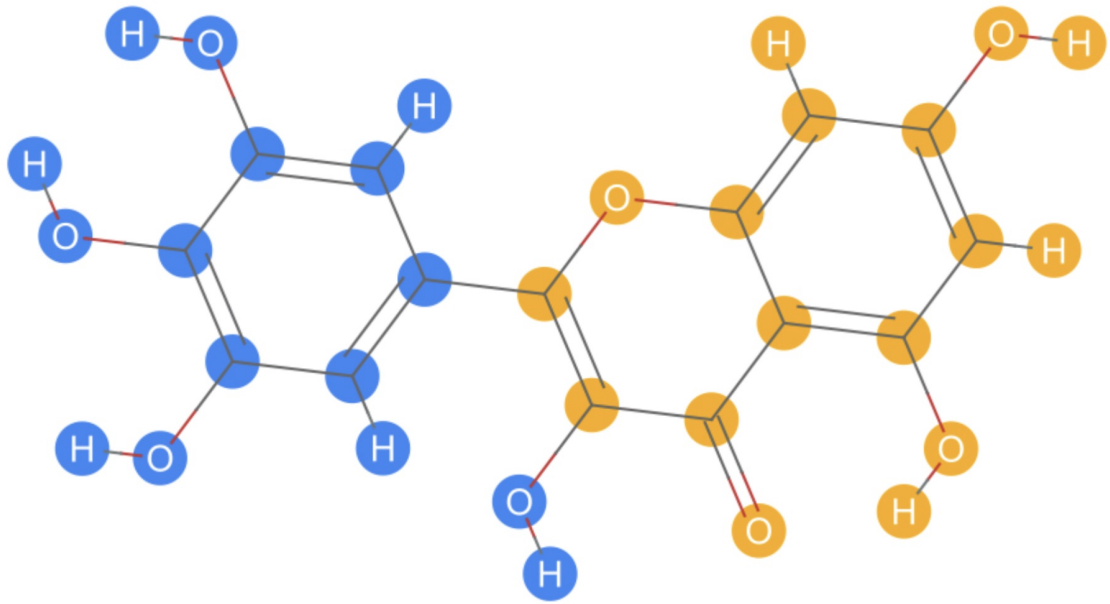


We say that N is robust regarding P if $\forall \bar{x}' \in B$ it holds $N(\bar{x}) = N(\bar{x}')$.

Neural Models for Graph-Data



(1) social networks

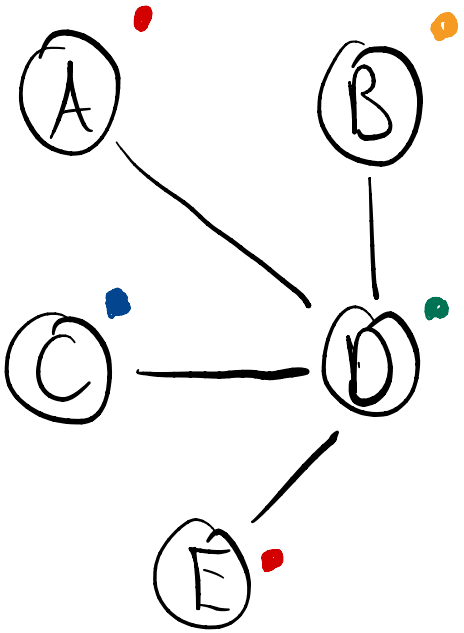


(2) molecule classification

(1) Cuk Baek, 2022
(2) wolfram.com

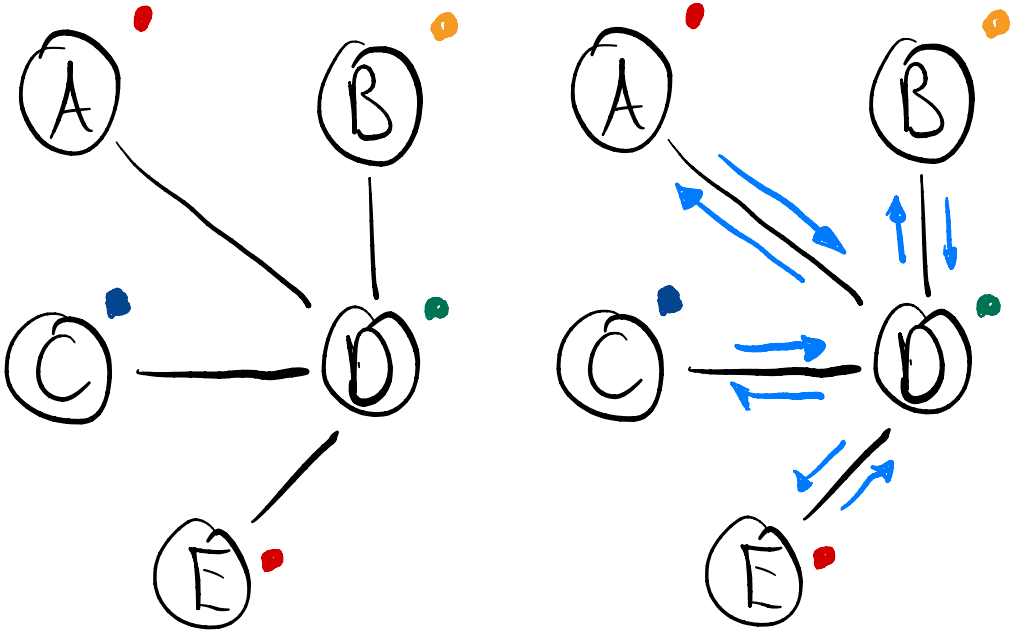
Graph Neural Networks (GNN)

Usual model: Message-Passing or Aggregation-Combine



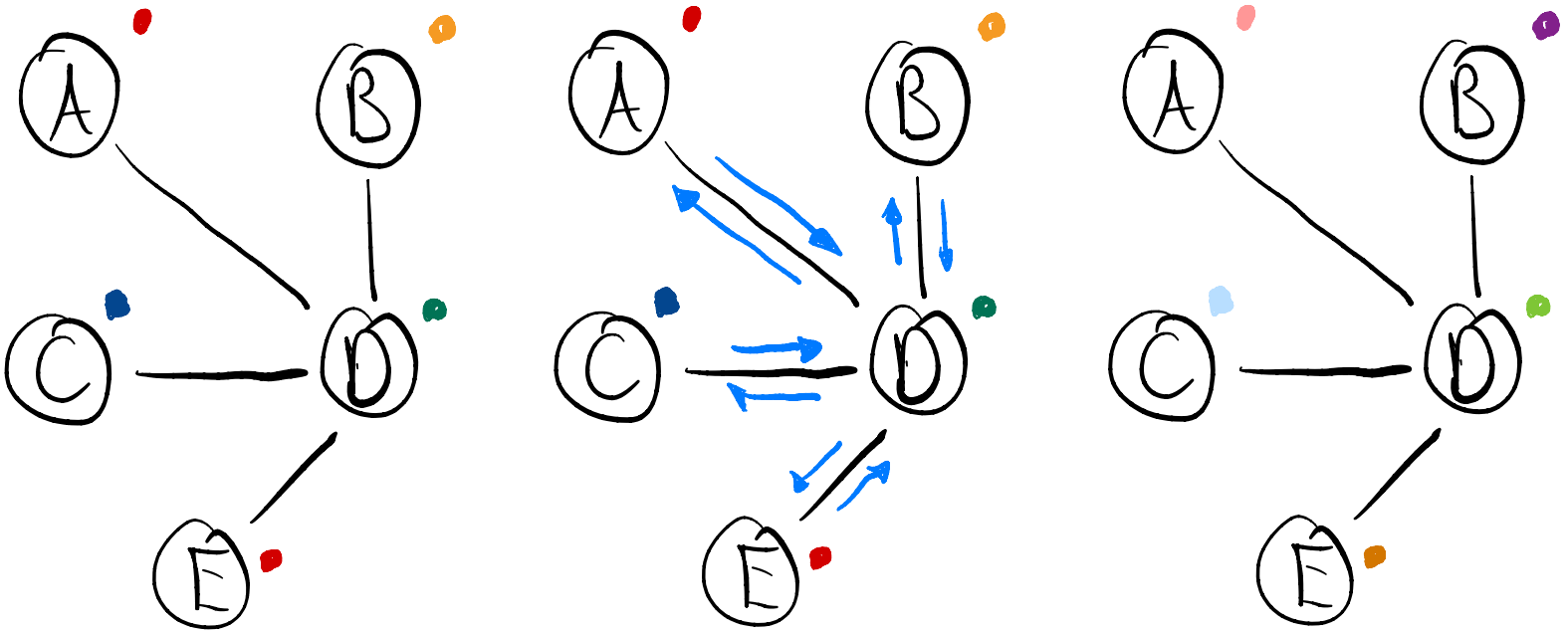
Graph Neural Networks (GNN)

Usual model: Message-Passing or Aggregation-Combine



Graph Neural Networks (GNN)

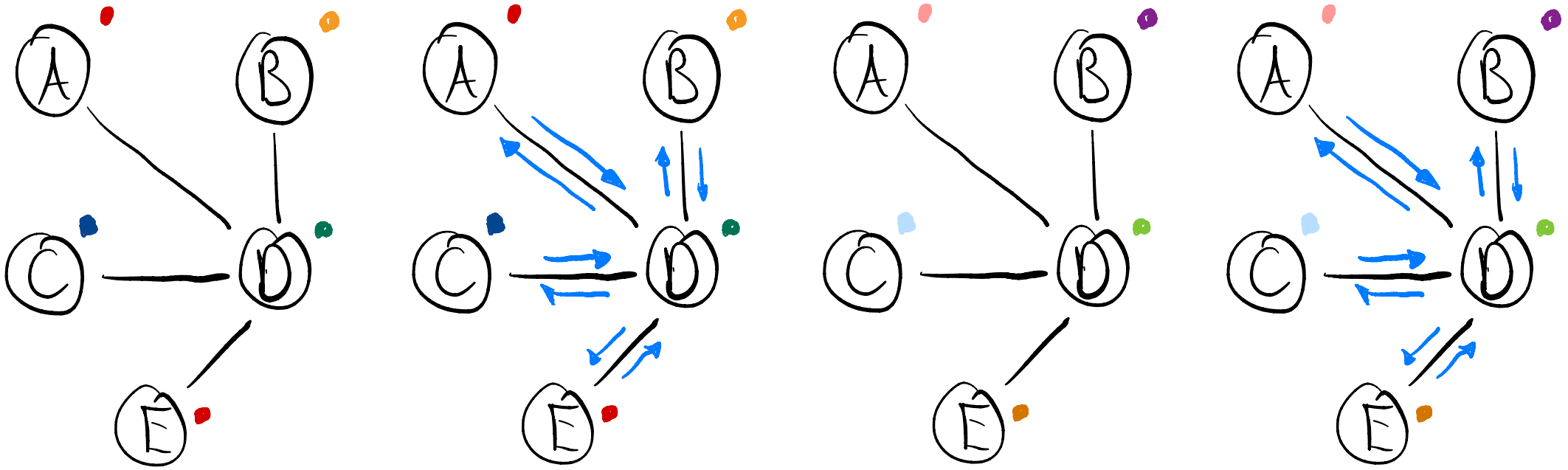
Usual model: Message-Passing or Aggregation-Combine



$$\bar{X}_v^{i+1} = \text{comb}\left(\bar{x}_i, \text{agg}\left(\{\{\bar{x}_u^i \mid u \in \text{neigh}(v)\}\}\right)\right)$$

Graph Neural Networks (GNN)

Usual model: Message-Passing or Aggregation-Combine

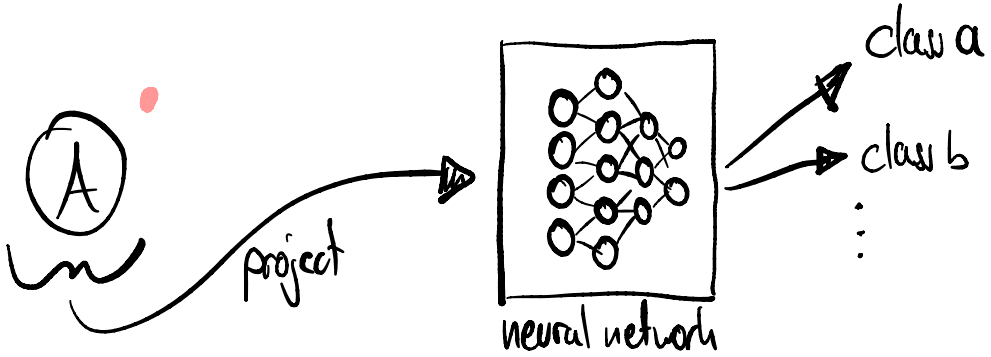


$$\bar{X}_v^{i+1} = \text{comb}\left(\bar{x}_i, \text{agg}\left(\{\{\bar{x}_u^i \mid u \in \text{neigh}(v)\}\}\right)\right)$$

Graph Neural Networks (GNN)

Usual tasks:

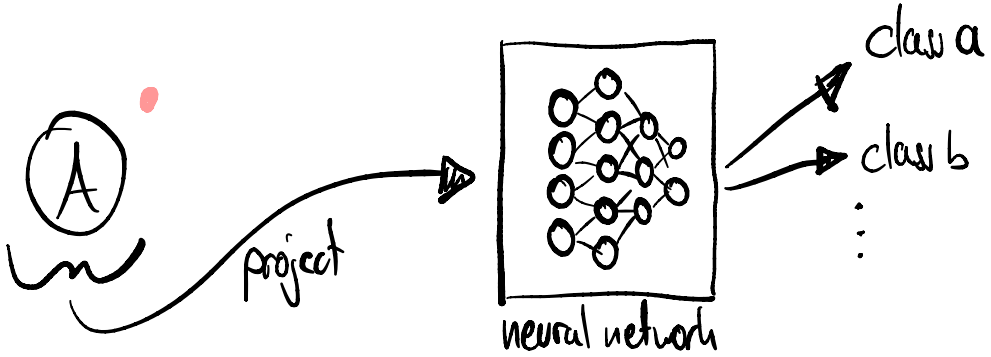
node classification



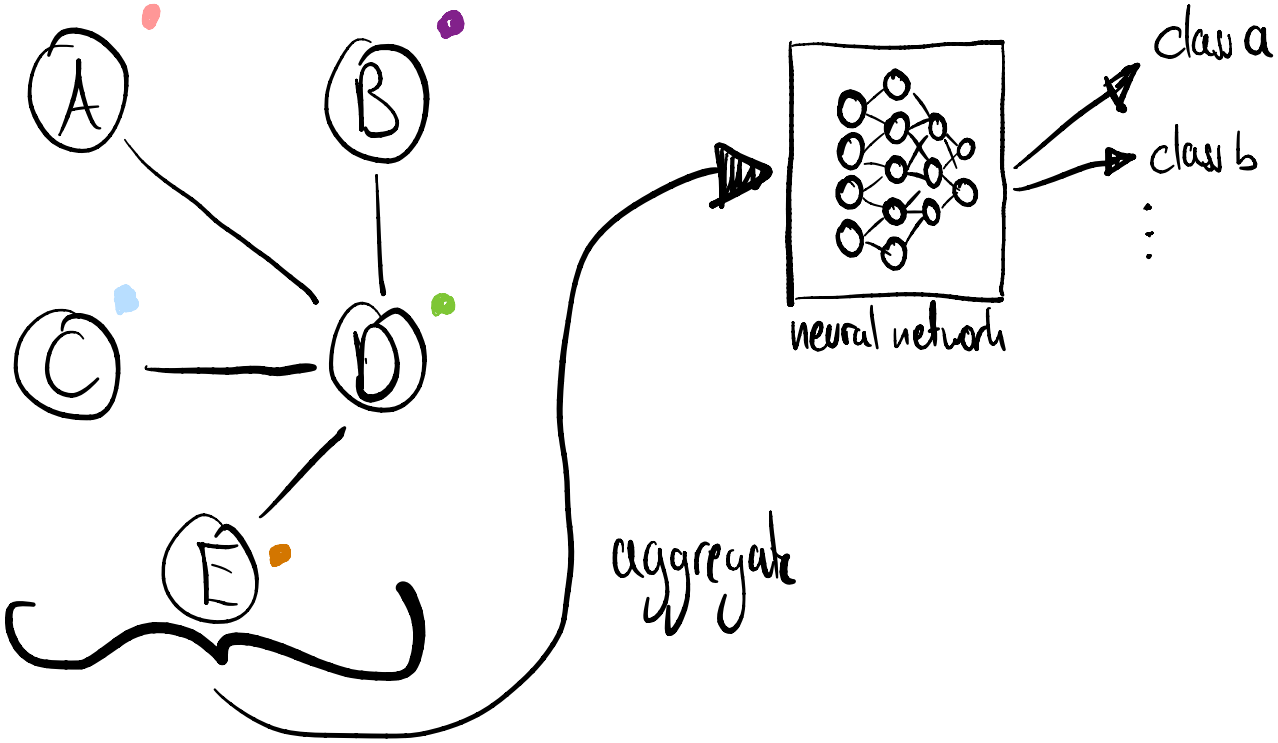
Graph Neural Networks (GNN)

Usual tasks:

node classification



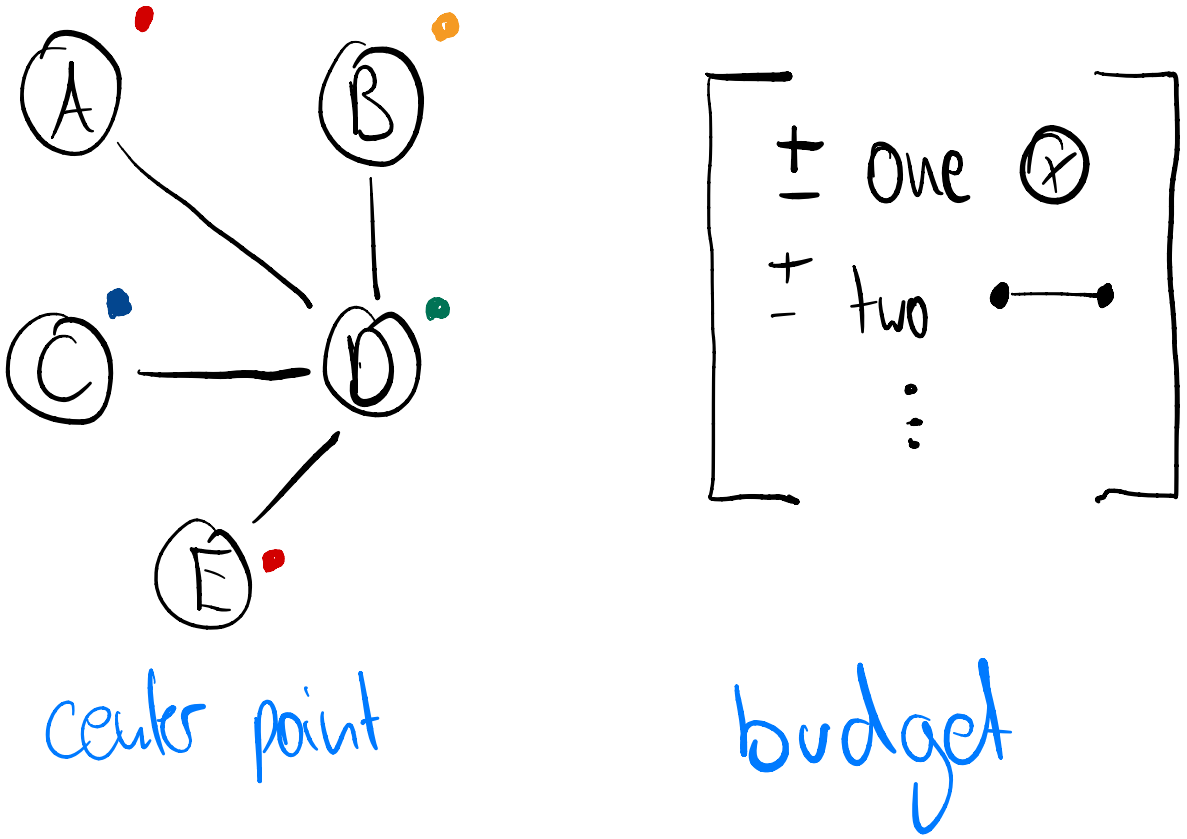
whole graph classification



Point-wise Robustness over Graph Data

Analogous to real-valued data. Center point is some graph G and budget are allowed amount of perturbations.

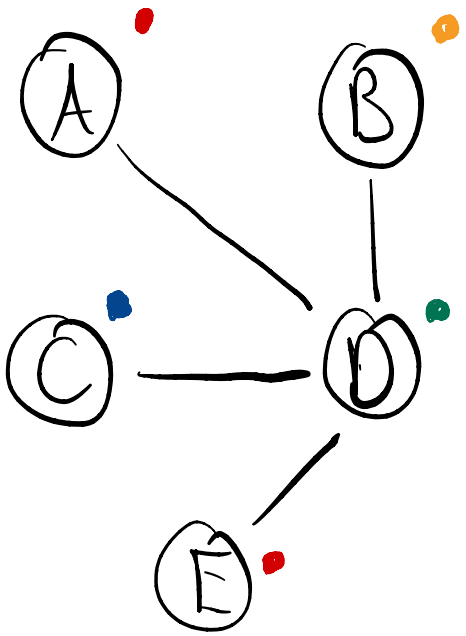
Example:



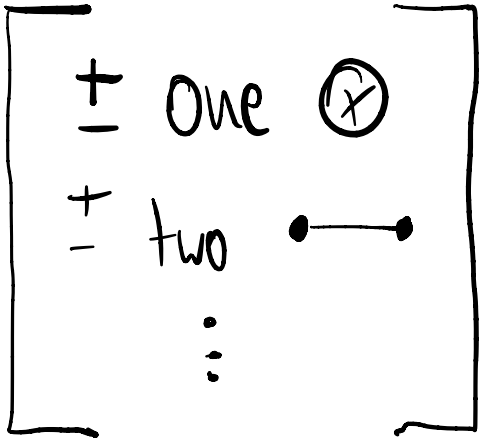
Point-wise Robustness over Graph Data

Analogous to real-valued data. Center point is some graph G and budget are allowed amount of perturbations.

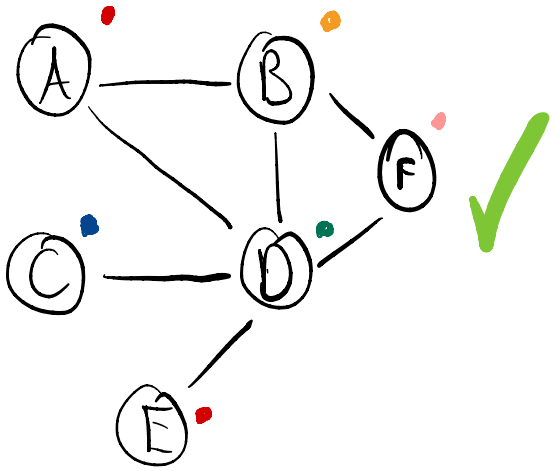
Example:



center point



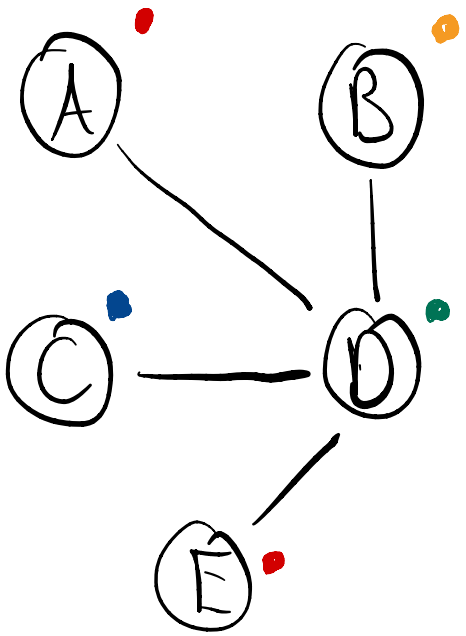
budget



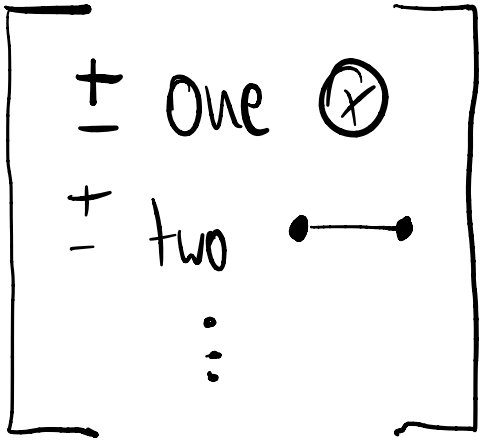
Point-wise Robustness over Graph Data

Analogous to real-valued data. Center point is some graph G and budget are allowed amount of perturbations.

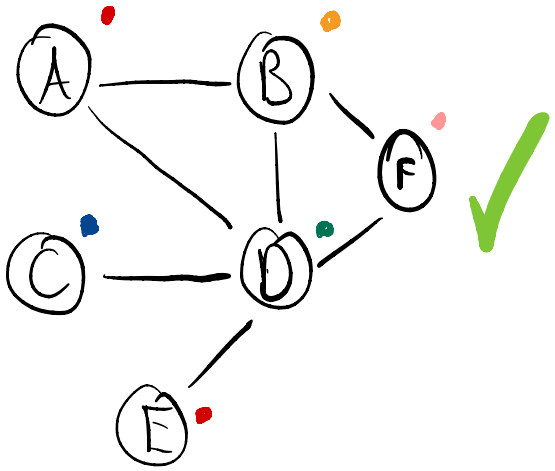
Example:

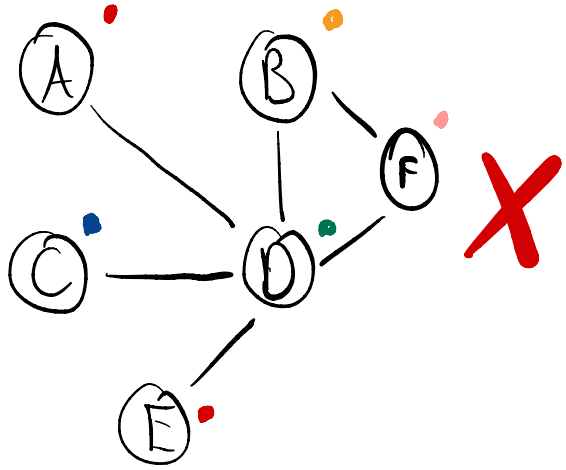


center point

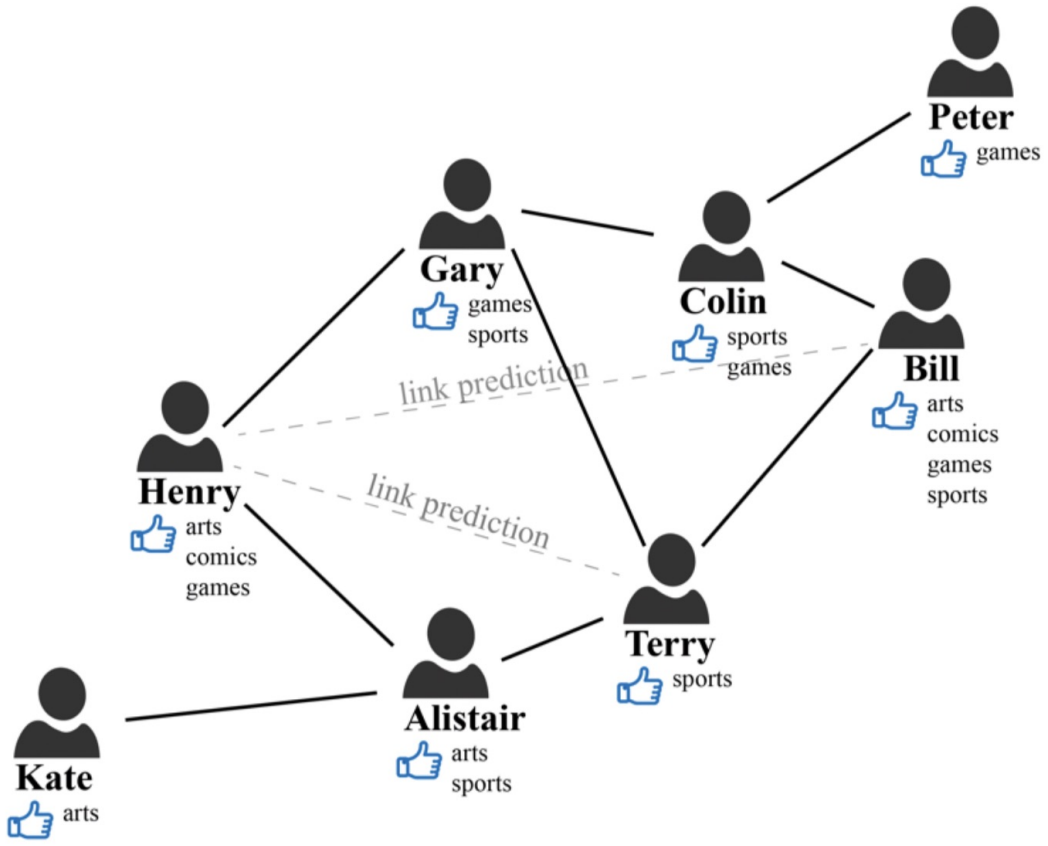


budget

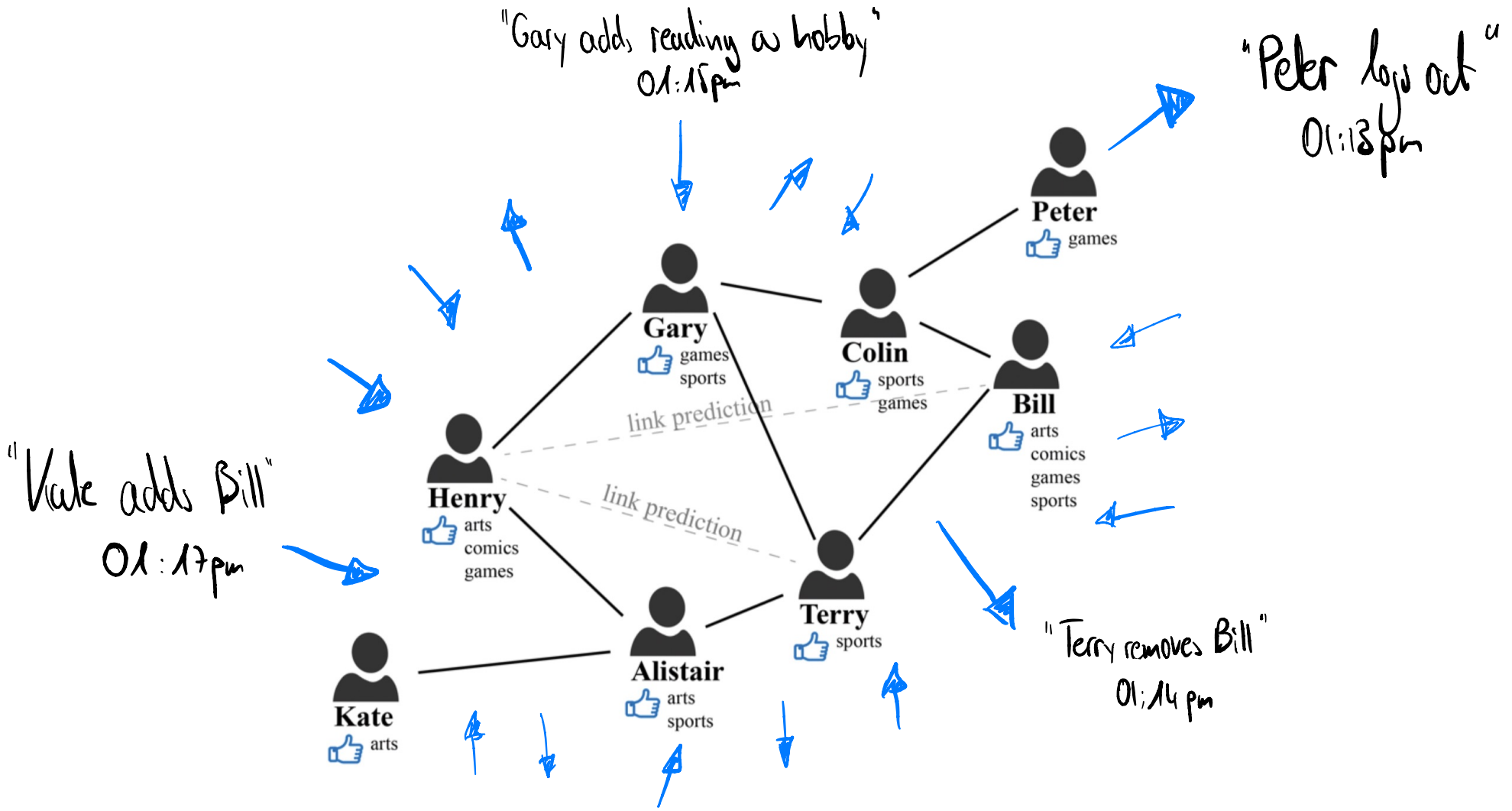




Limitations of the Usual GNN Setting



Limitations of the Usual GNN Setting



Temporal Graph Neural Networks (TGNN)

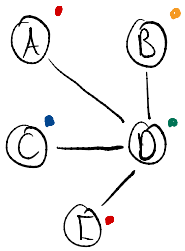
A Continuous-Time Temporal Graph (CTG) is a tuple (G, O)

- G is a (usual) graph, called start graph
- O is a (finite) set of time-stamped observations

Temporal Graph Neural Networks (TGNN)

A Continuous-Time Temporal Graph (CTG) is a tuple (G, O)

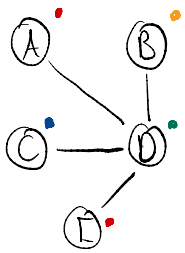
- G is a (usual) graph, called start graph
- O is a (finite) set of time-stamped observations

$$\left(\text{  }, \{(t_1, \text{add}, F), (t_2, \text{add}, (D, F)), \ldots\} \right)$$

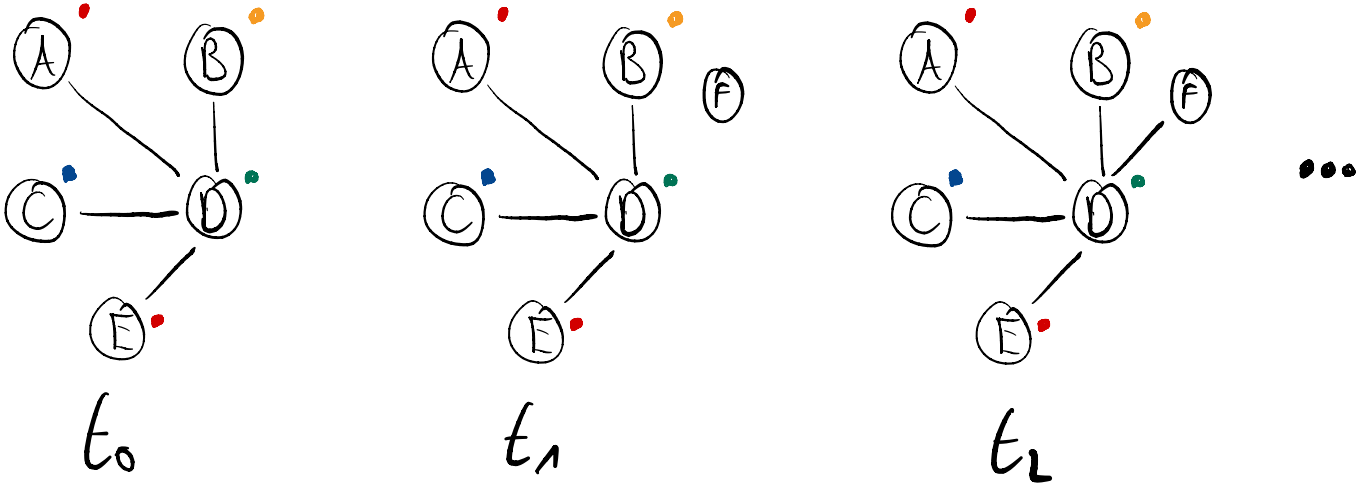
Temporal Graph Neural Networks (TGNN)

A Continuous-Time Temporal Graph (CTG) is a tuple (G, O)

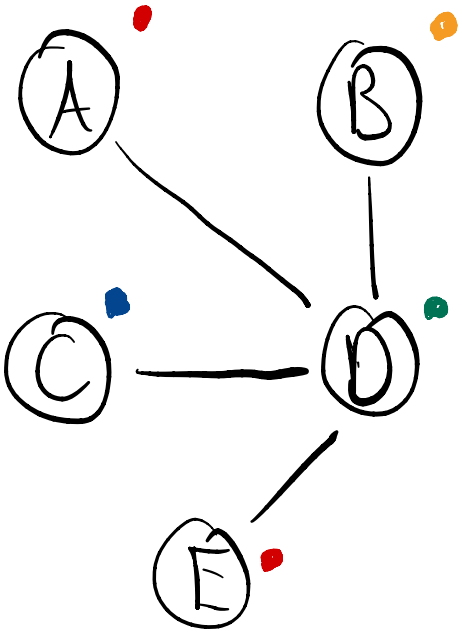
- G is a (usual) graph, called start graph
- O is a (finite) set of time-stamped observations

$$\left(\text{  }, \{(t_1, \text{add}, F), (t_2, \text{add}, (D, F)), \ldots\} \right)$$

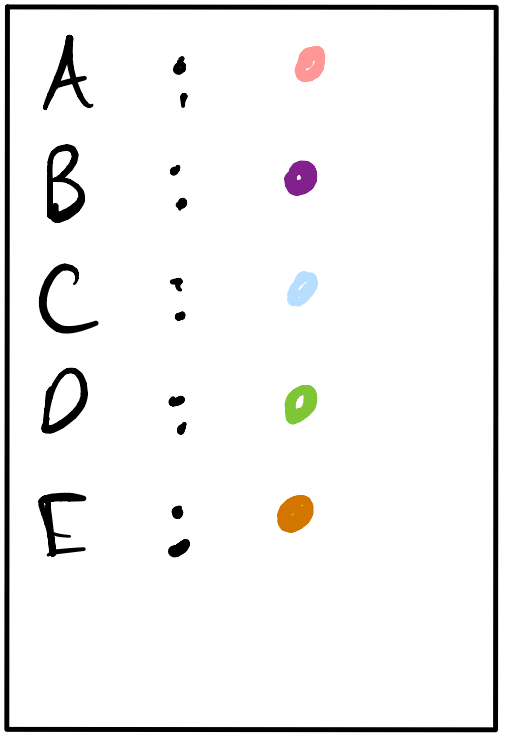
unfold



Temporal Graph Neural Networks (TGNN)

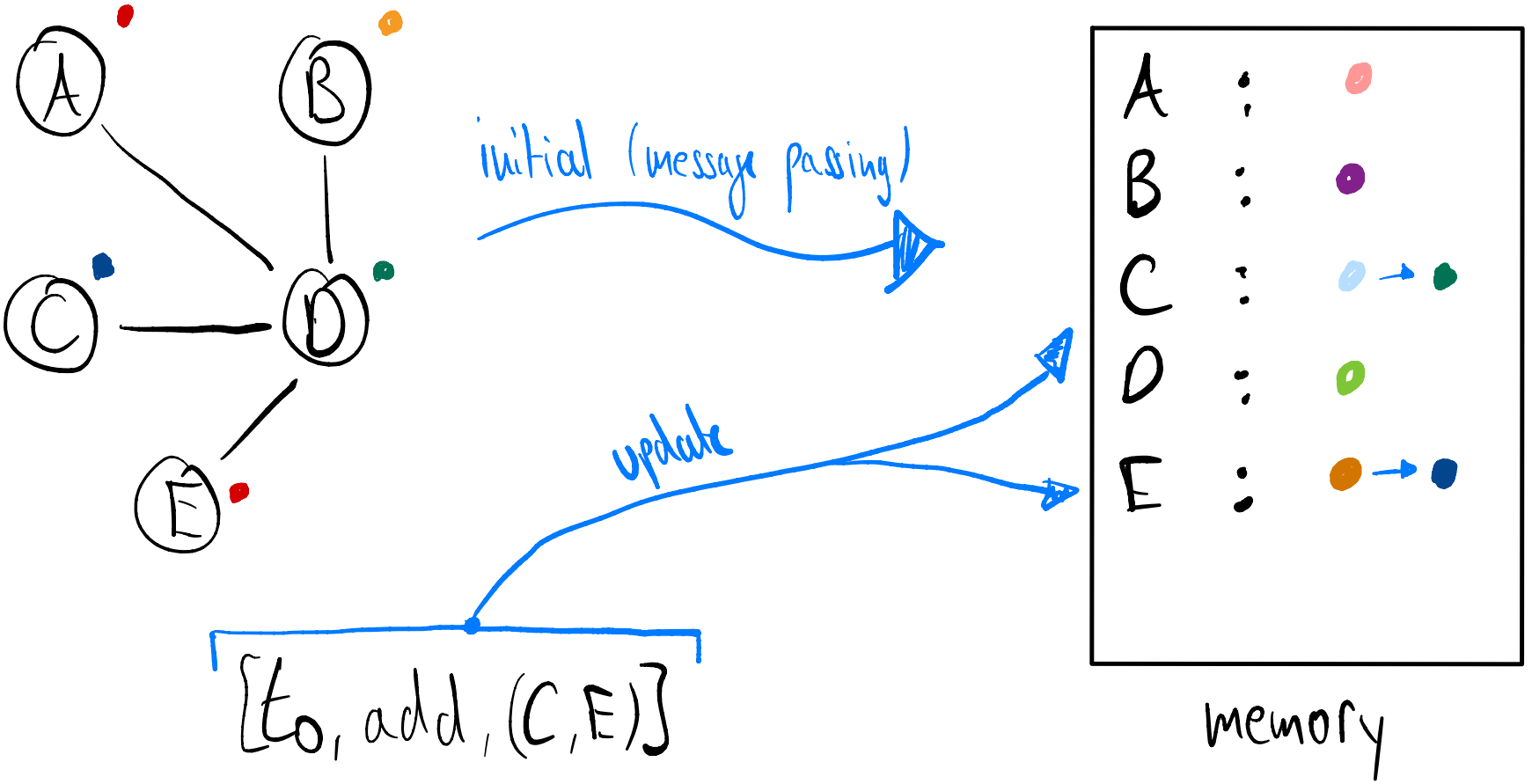


initial (message passing)

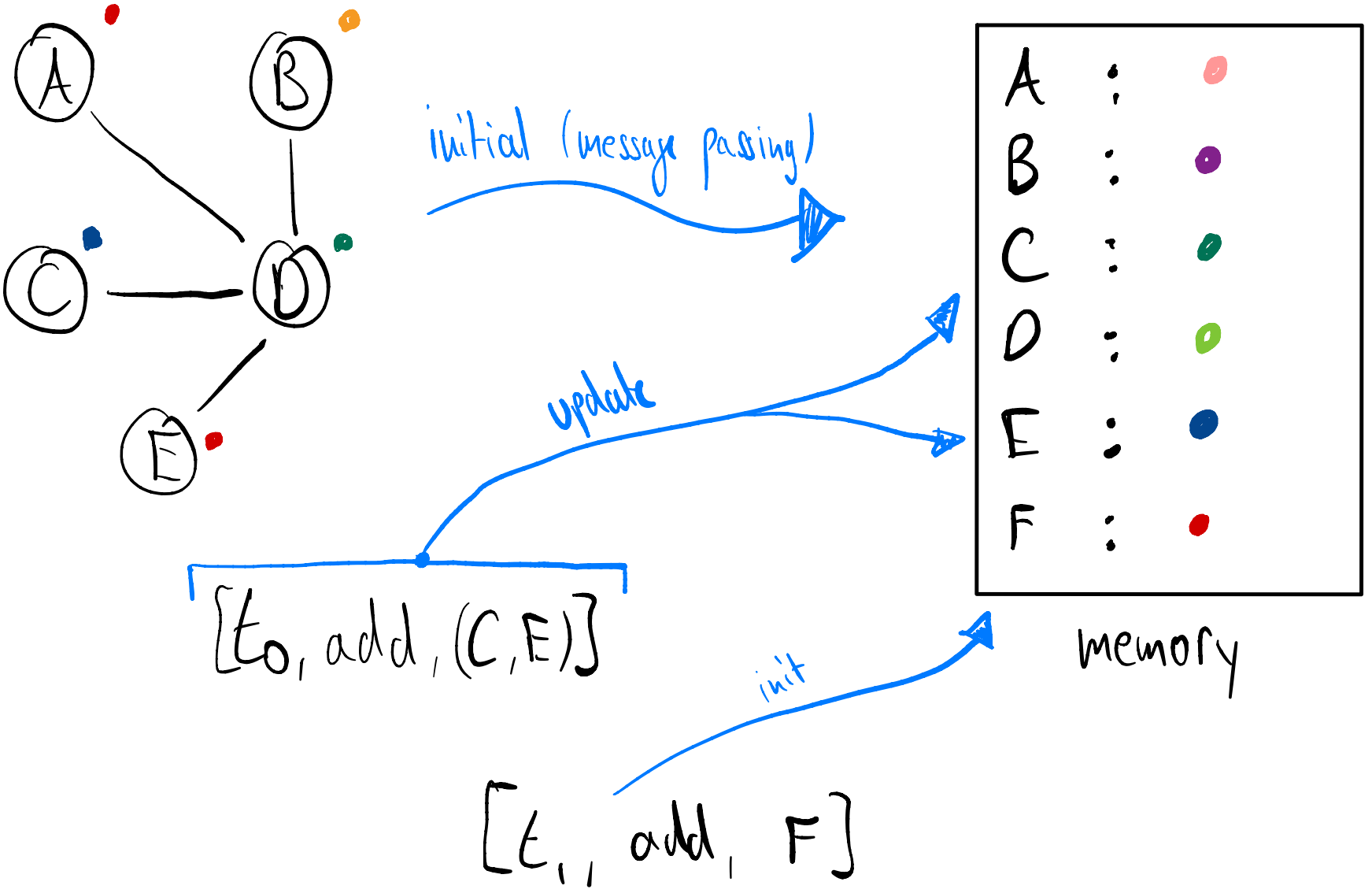


memory

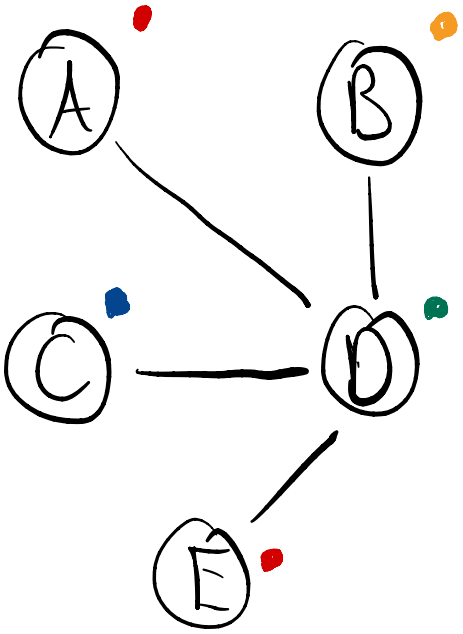
Temporal Graph Neural Networks (TGNN)



Temporal Graph Neural Networks (TGNN)



Temporal Graph Neural Networks (TGNN)



initial (message passing)

update

$[t_0, add, (C, E)]$

init

$[t_1, add, F]$

memory

A :
B :
C :
D :
E :
F :

continuous updates

$[t_2, add, (B, F)]$ ...

Temporal Graph Neural Networks (TGNN)

Usual tasks:

- same as GNN but time dependent: "class at time t?"

Temporal Graph Neural Networks (TGNN)

Usual tasks:

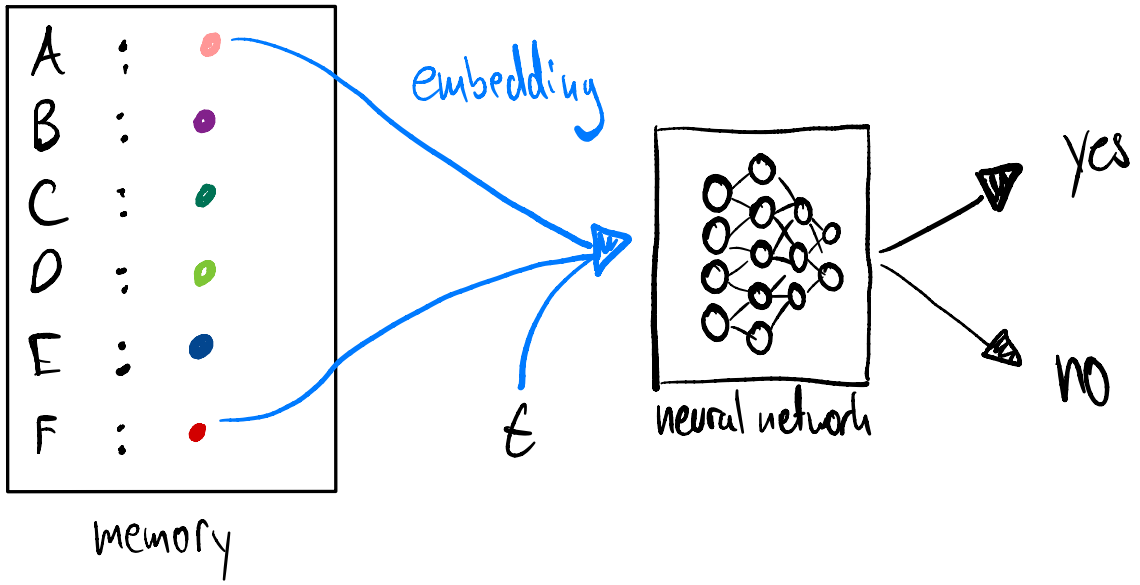
- same as GNN but time dependent: "class at time t ?"
- future link/edge prediction:
  given CTG (G, O) and nodes u, v present at time t_0:
  decide whether (u, v) edge is present at time $t \geq t_0$

Temporal Graph Neural Networks (TGNN)

Usual tasks:

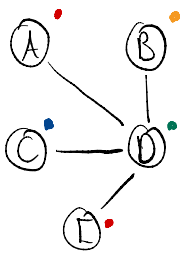
- same as GNN but time dependent: "class at time t ?"
- future link/edge prediction:

  given CTG (G, O) and nodes u, v present at time t_0.
  Decide whether (u, v) edge is present at time $t \geq t_0$



What about Robustness of TGNN?

Point-wise Robustness for Link Prediction over CTG

$$\left(\text{  }, \{(t_1, \text{add}, F), \dots\} \right)$$

center point

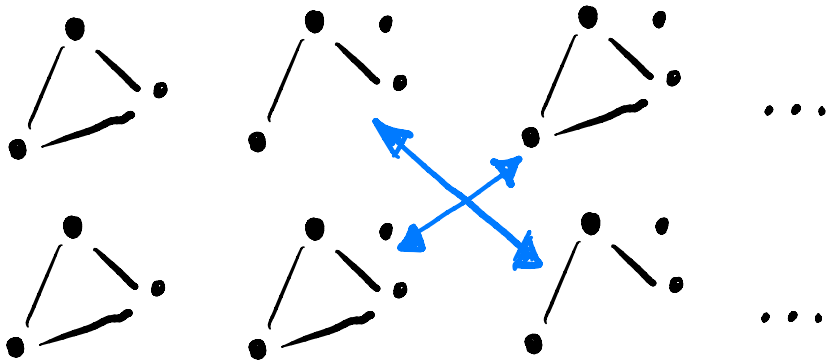
$$\left[\{(t_i', \text{add}, G), \dots\}, \{(t_j, \text{add}, (A,B)), \dots\} \right]$$

budget

"additions" "deletions"

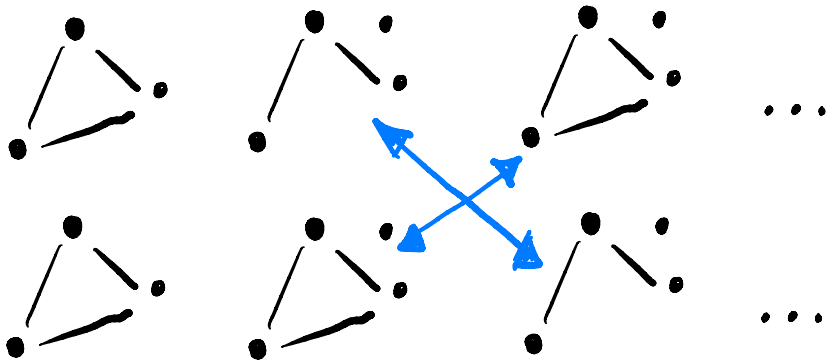
We say that TGNN N is robust for nodes u, v at time t regarding P if for all $C' \in P$ ...

Some Thoughts on Similar CTG

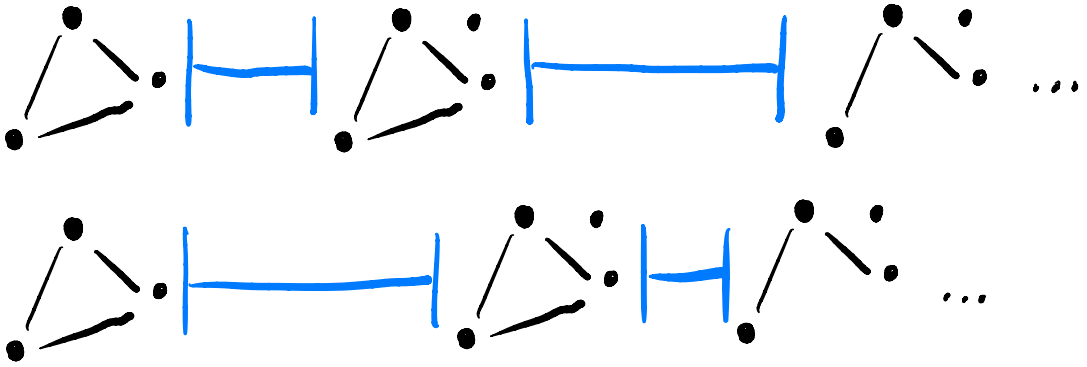


rotations

Some Thoughts on Similar CTG



rotations



time shifts

⋮

Conclusion / Outlook

- Temporal Graph Neural Networks lack robustness verification methods

Conclusion / Outlook

- Temporal Graph Neural Networks lack robustness verification methods
- What are meaningful measures of similarity for temporal graphs?

Conclusion / Outlook

- Temporal Graph Neural Networks lack robustness verification methods
- What are meaningful measures of similarity for temporal graphs?
- Desirable: finding ways to integrate existing research on temporal properties

Conclusion / Outlook

- Temporal Graph Neural Networks lack robustness verification methods
- What are meaningful measures of similarity for temporal graphs?
- Desireable: finding ways to integrate existing research on temporal properties

Thanks!