Metagraphs, Policy and Security in Comms Networks

Prof Matthew Roughan
University of Adelaide
<matthew.roughan@adelaide.edu.au>

THE UNIVERSITY of ADELAIDE

TELETRAFFIC RESEARCH CENTRE

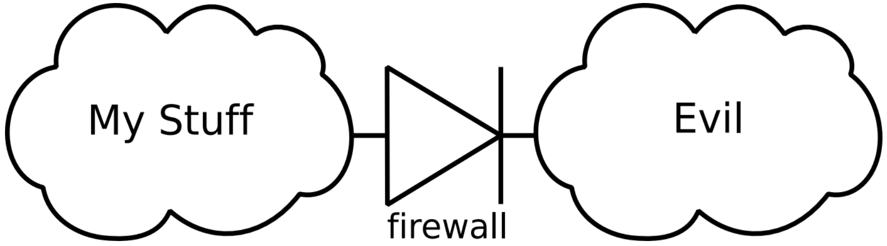
Thanks

- Lots of people have been involved
- Uni of Adelaide
  - Eric Parsonage
  - Hung Nguyen
  - Dinesha Ranathunga
  - +++
- DST folks
  - Kelly Kapsabelis
  - Robert McAuley
  - James Biddle
  - +++

Why is Cybersecurity SO SO Hard

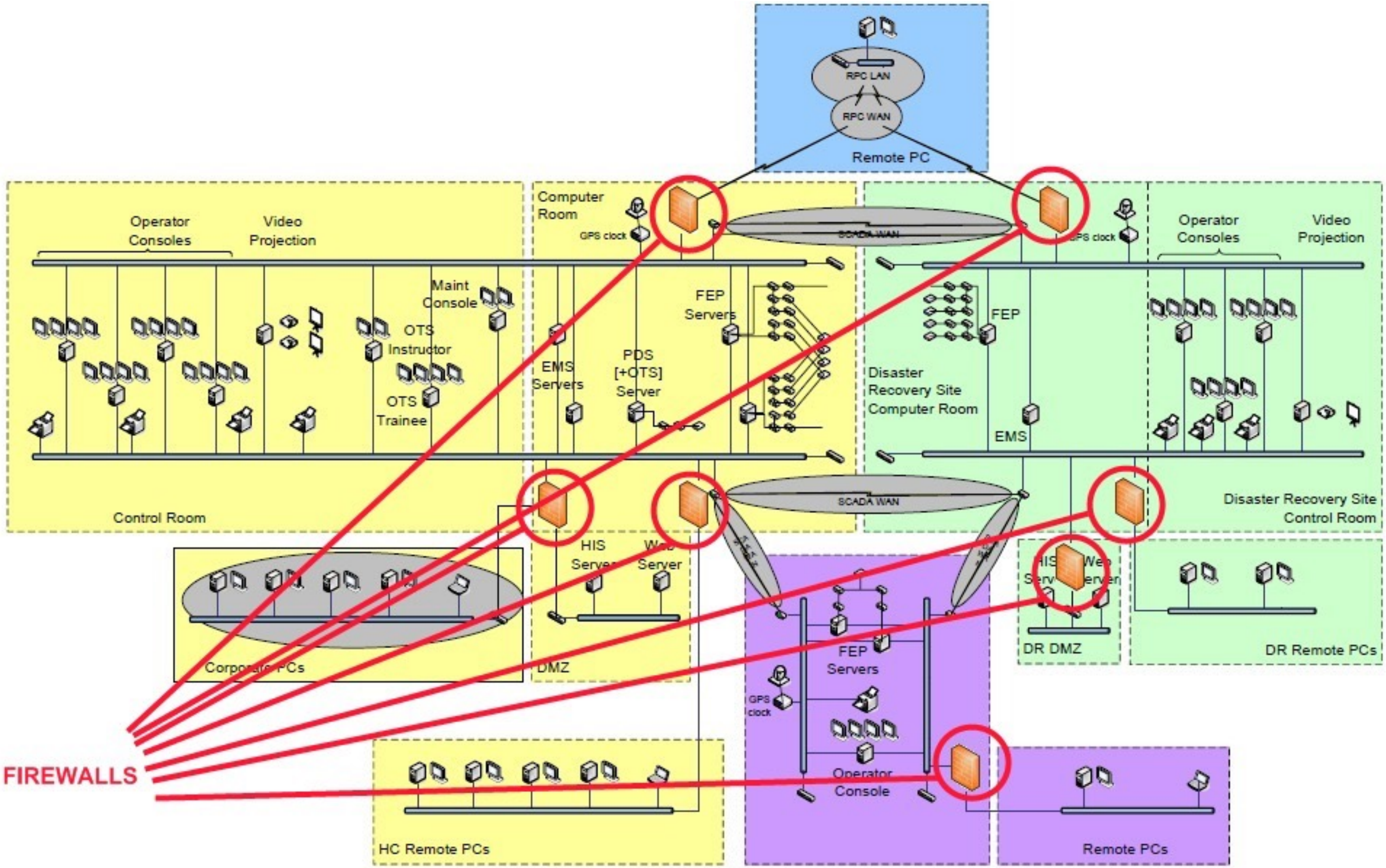
- Communications networks are big and complicated
  - 10's of thousands of devices are common
    - They are multi-layered, heterogenous, distributed, ...
  - The protocols that keep them running involve complex dynamics, and many interactions
  - The rules that create a cybersecurity policy are MANY
  - There is no way a human can reason about the system without help
- But there is a difference between complex and complicated
  - Some of the problems in this space are just complicated

For example – Adelaide Uni's Net



- **The network has**
  - 2 types of firewall
  - Well over 2 million rules, distributed over hundreds of devices
    - Access control
    - Anti-malware
    - Anti-spyware
    - URL-filtering
    - Reporting
- **Mistakes**
  - ~500 conflicting rules
  - ~1000 redundancies

Real power stations in Oz:
9 out of 9 had mistakes and these networks were actually simpler (and more important) than UofA's "corporate" network.



RPC LAN
RPC WAN
Remote PC
Computer Room
GPS clock
SCADA WAN
Operator Consoles
Video Projection
Maint Console
FEP Servers
OTS Instructor
EMS Servers
PDS [+OTS] Server
OTS Trainee
Control Room
FEP
Disaster Recovery Site Computer Room
EMS
Disaster Recovery Site Control Room
HIS Server
Web Server
Corporate PCs
DMZ
DR DMZ
DR Remote PCs
FEP Servers
GPS clock
Operator Console
HC Remote PCs
Remote PCs
FIREWALLS

The single most important factor of your firewall's security is how you configure it.

Rubin and Greer

Reasoning about policy

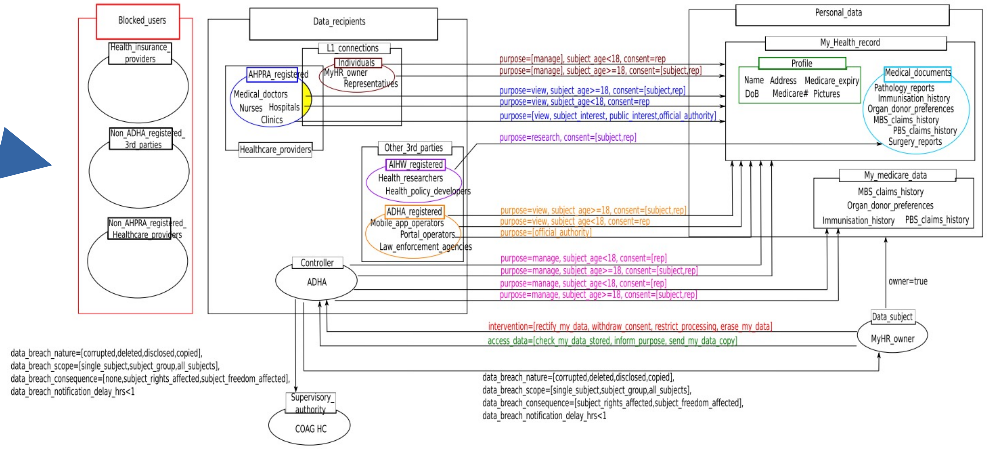
- **Compliance checking against standards like Australian Cyber Security Centre (ACSC) or NIST best practices**

  e.g., https://www.nist.gov/cybersecurity
- **Detecting and reasoning about exceptions,**

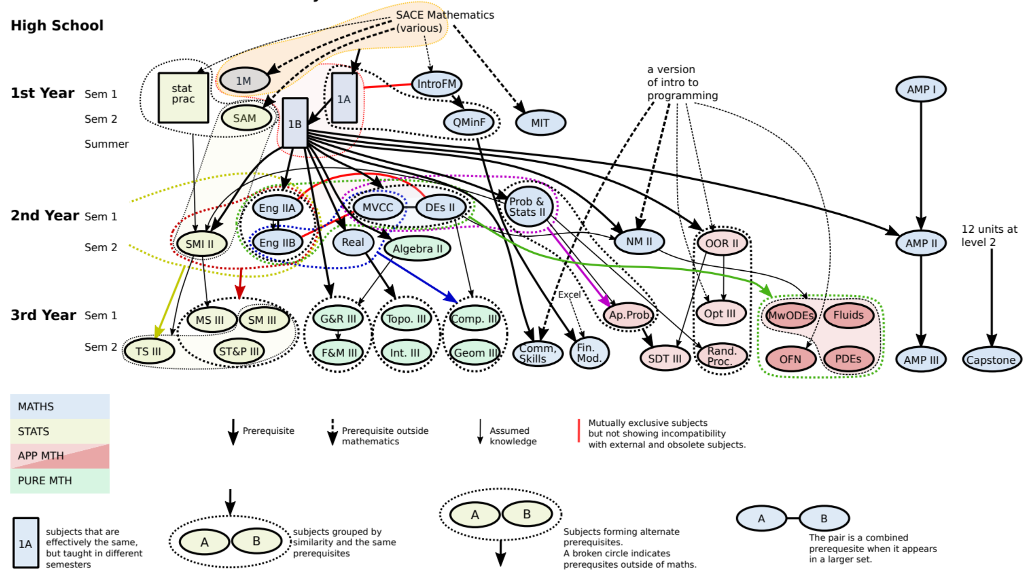
  e.g., careful risk analysis
- **Allowing A distributed team to share management of policy**
- **Maintaining consistent policy as network infrastructure changes**
- **Simplify – avoid making new vulnerabilities (e.g., CrowdStrike)**
- **Optimise**

Other Policy Problems

- Health Privacy Policy
- Education Pathways
- Supply Chains

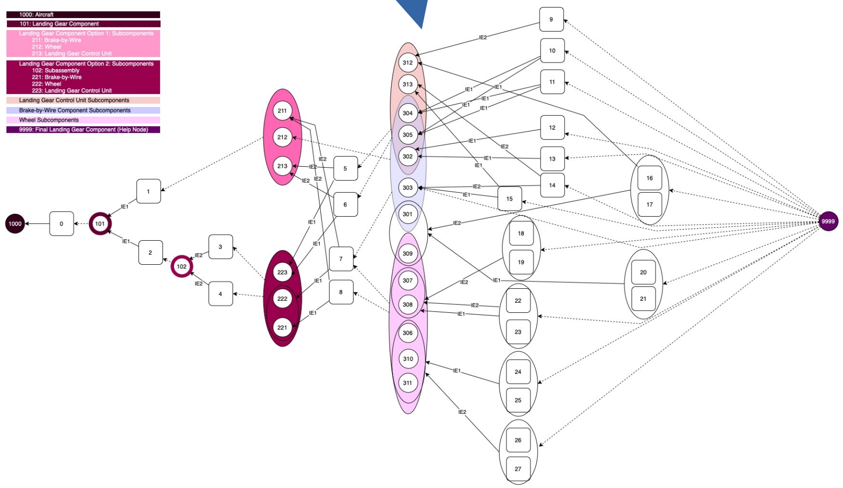


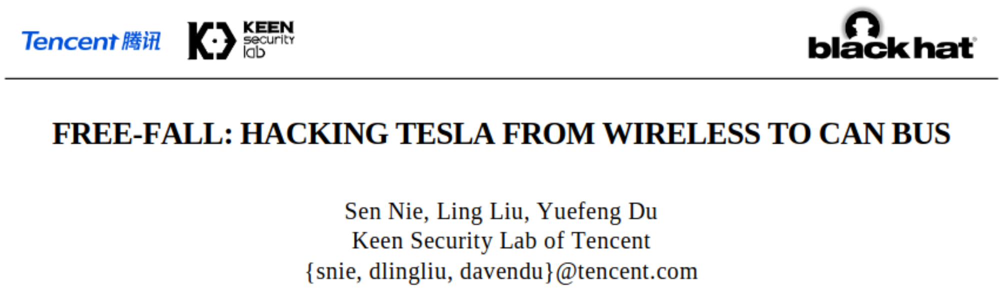
School of Mathematical Sciences subject "tree"



Construction rules
(1) Avoid prerequisite of 1st semester for 2nd
(2) Minimise prerequisites, in pref. to assumed
(3) Provide alternative pathways for engineers, etc.

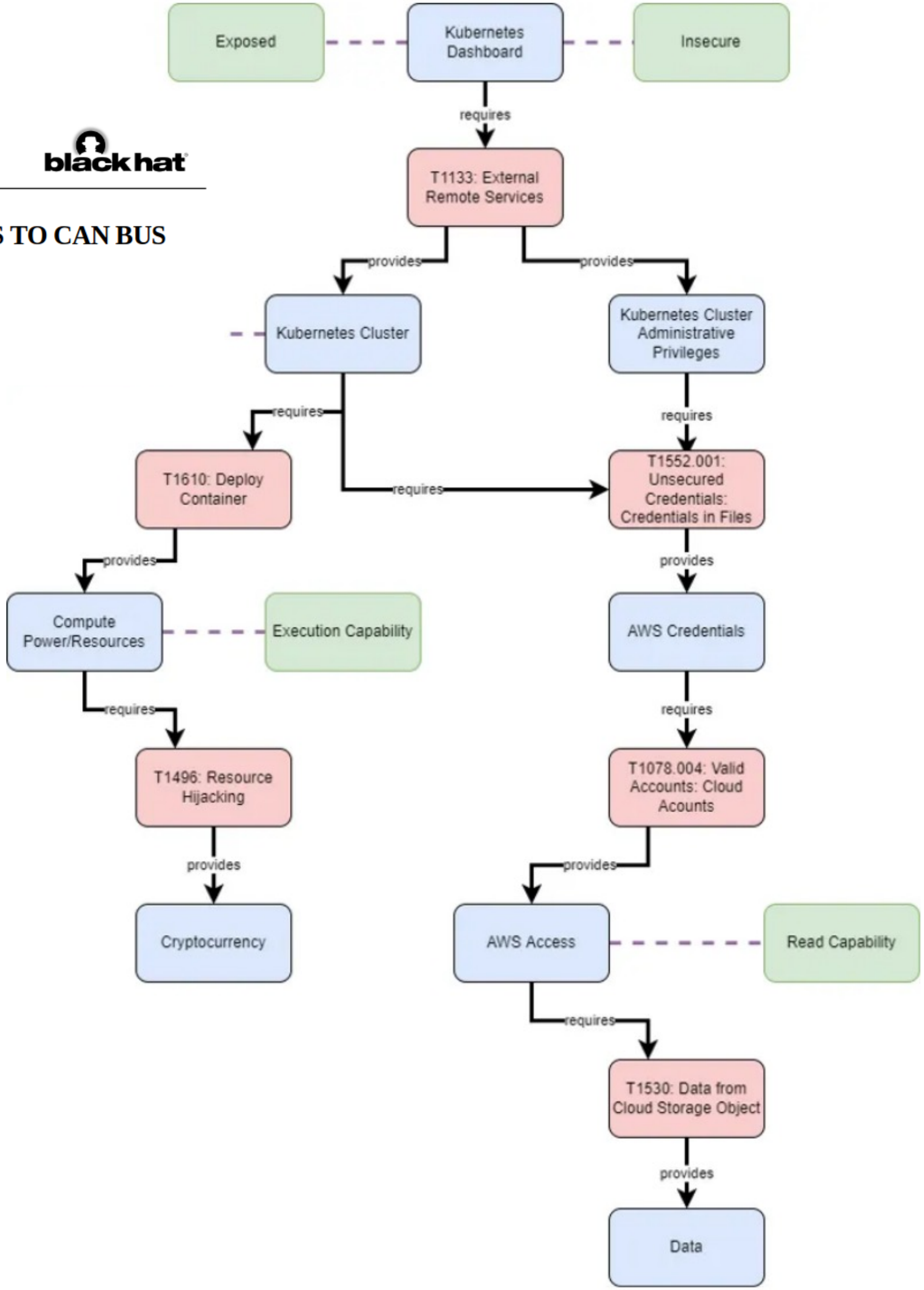
Tests
(1) does a set of subjects meet requirements
(2) does a set of subjects qualify for other criteria, e.g. majors
(3) what is the effect of failing X?
(4)




FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS

Sen Nie, Ling Liu, Yuefeng Du
Keen Security Lab of Tencent
{snie, dlingliu, davendu}@tencent.com

Attacks are Networks Too

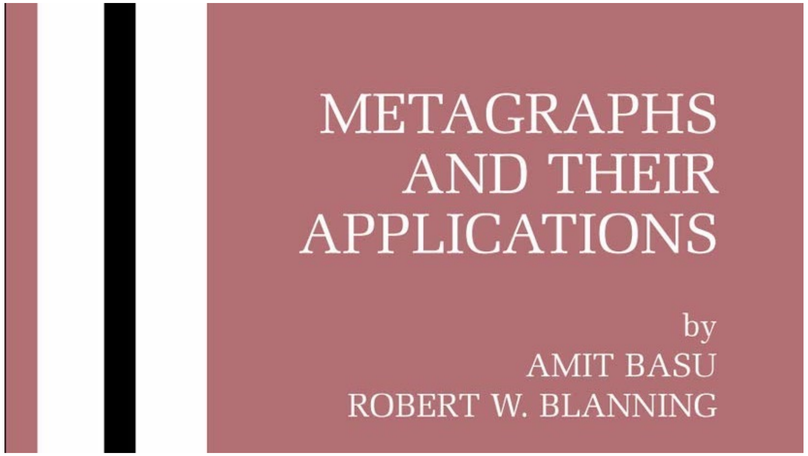


Key Ideas

- Use formal methods to help people reason about these complex systems
  - Typically, formal = logic
  - For me, formal = Math (graph theory, algebra, ...) + CS (algorithms, compilers, …)
- Systems have to
  - Work with real data (real networks, real protocols, ...)
  - Cope with large scale
  - Separate concerns (policy is not technology)

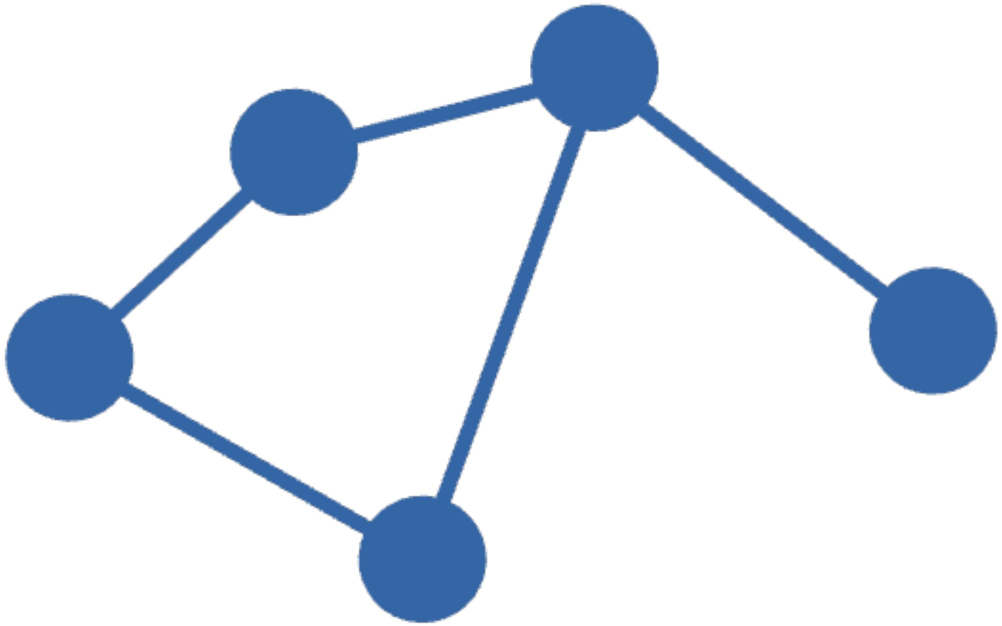
metagraphs

What is a metagraph?



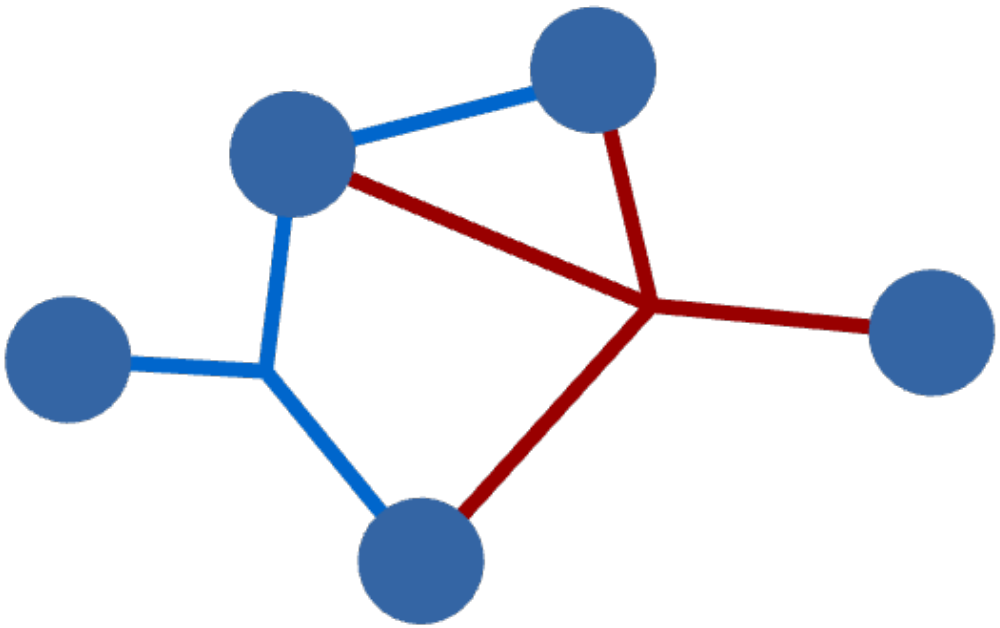
A simple graph shows relationships between pairs of

- Nodes
- Actors
- Entities
- Vertices



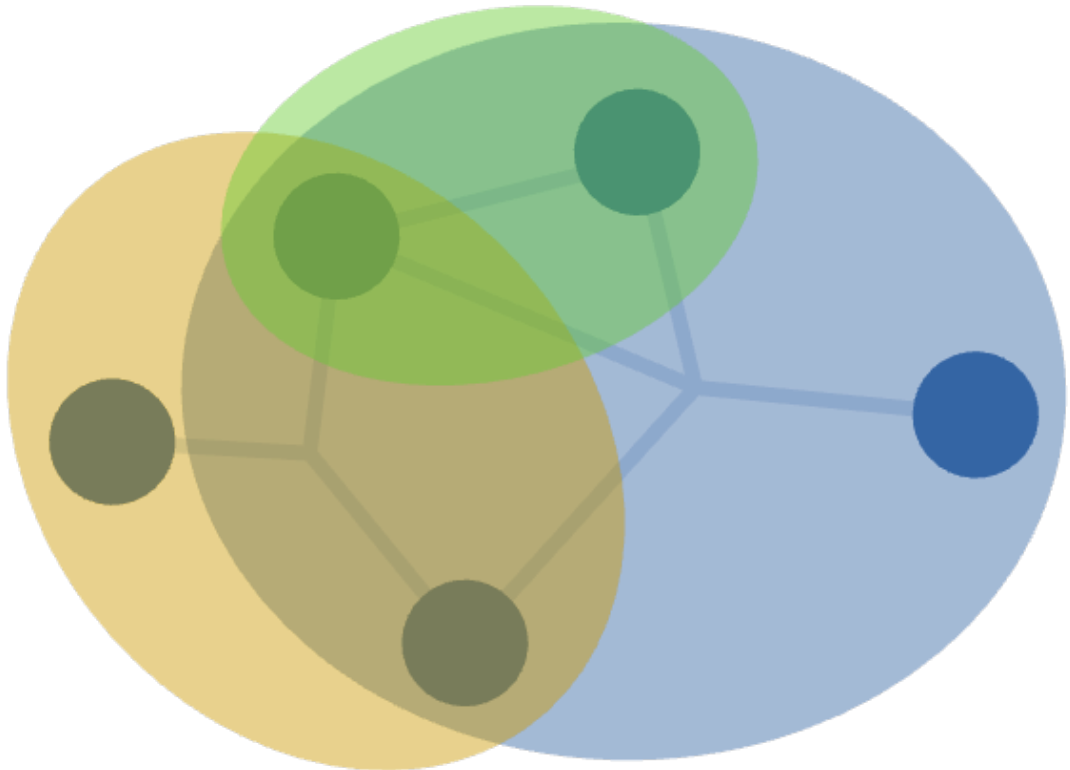
What is a metagraph?

A hypergraph shows multi-way relationships between nodes



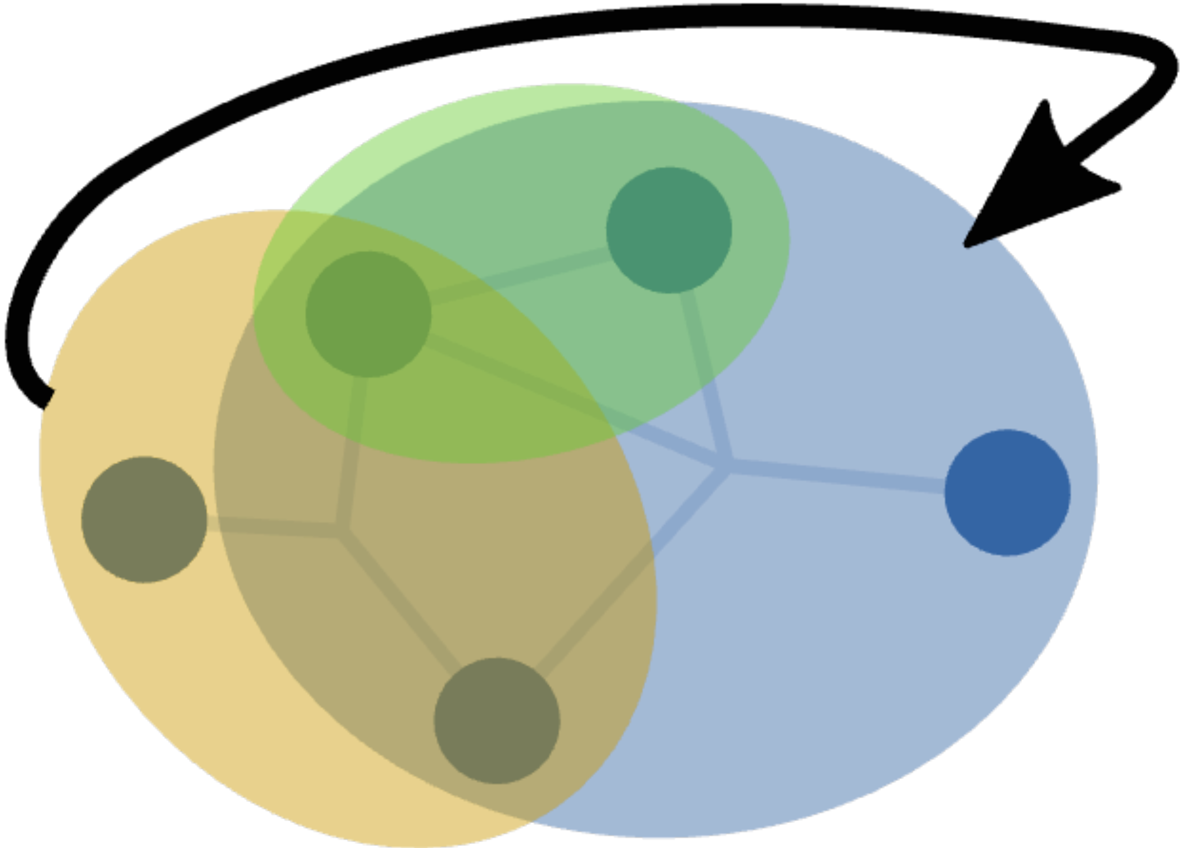
What is a metagraph?

We can think of a hypergraph as defining groups or sets



What is a metagraph?

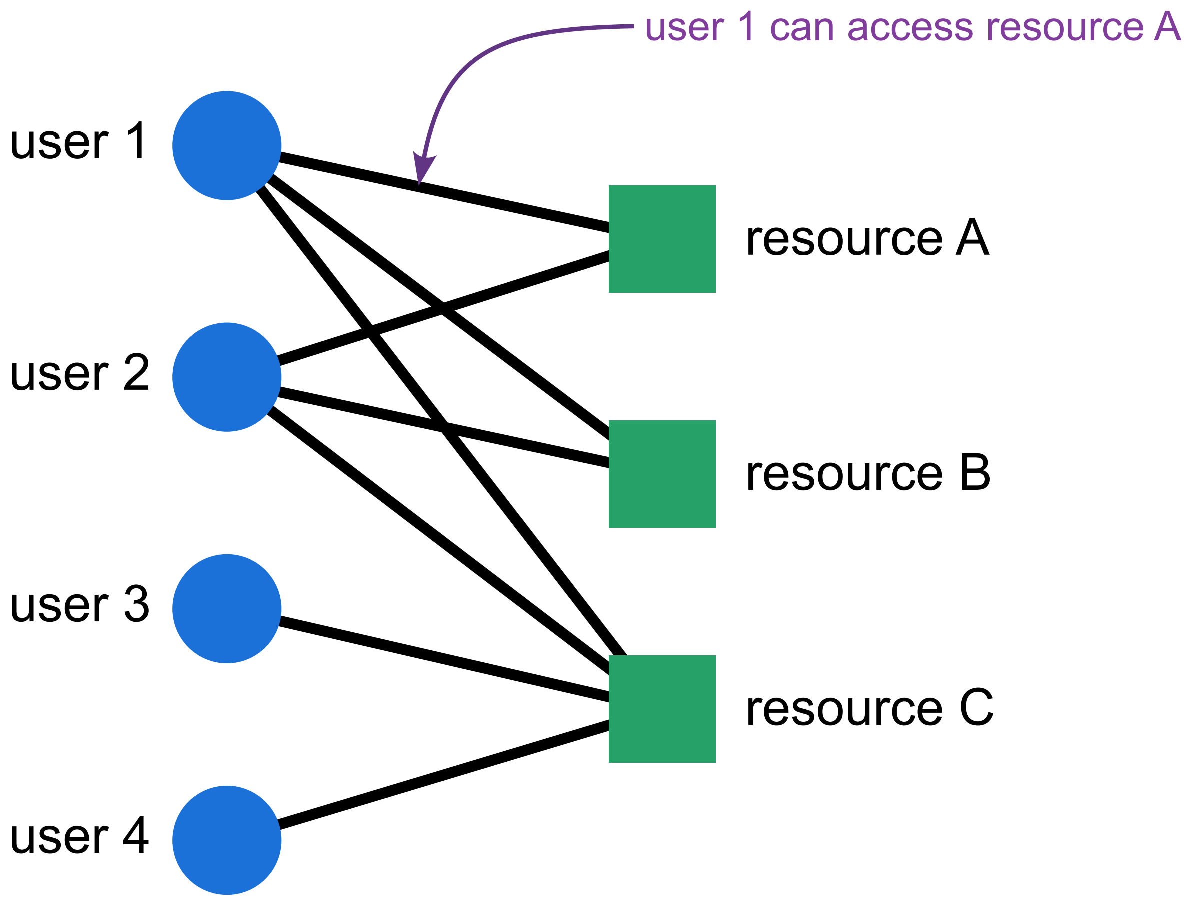
A metagraph shows (directed) relationships between these sets



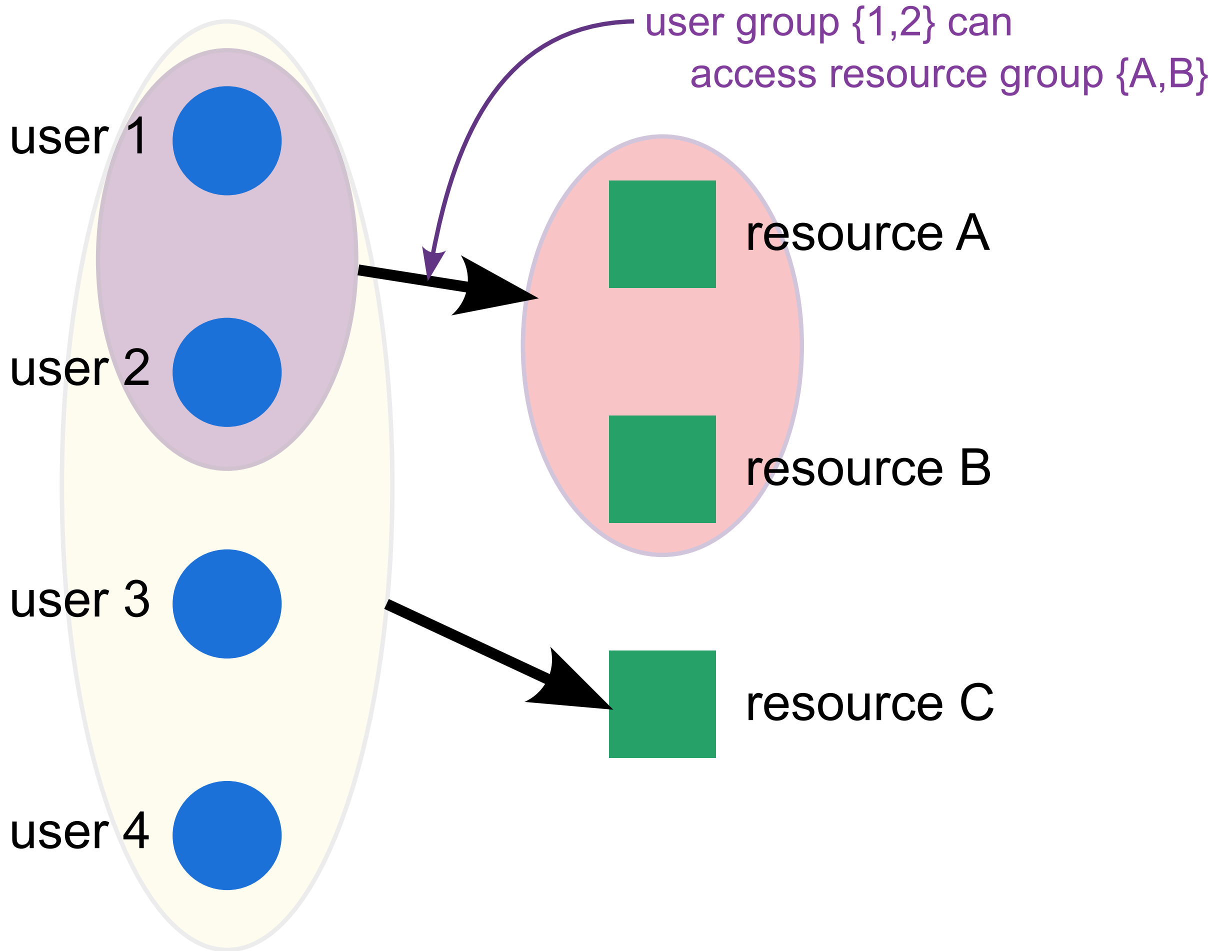
In reality a directed hypergraph is almost the same thing, but the terminology is useful

Why Metagraphs?

Simple graph policy network



Simple graph policy network

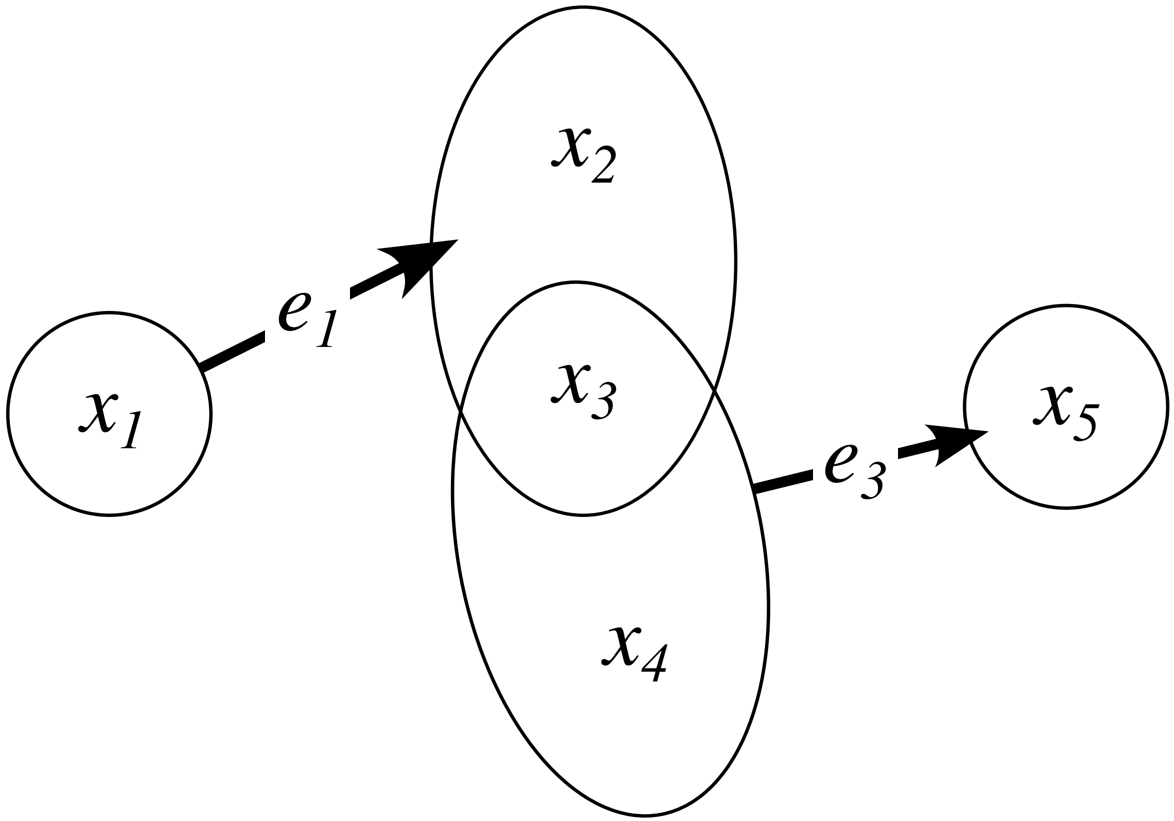


Why Metagraphs?

- Complexity of graphs grows rapidly
  - # edges might be huge – we just see spaghetti
- Often, actors in a graph are equivalent
- Often, relationships are naturally between groups
  - So it's more natural to represent complex interactions using a metagraph
- Separates policy from details
  - I don't need to name all of my "users" to describe a policy
- Plus: we have a few constructions with metagraphs that don't exist for graphs
  - Metapaths

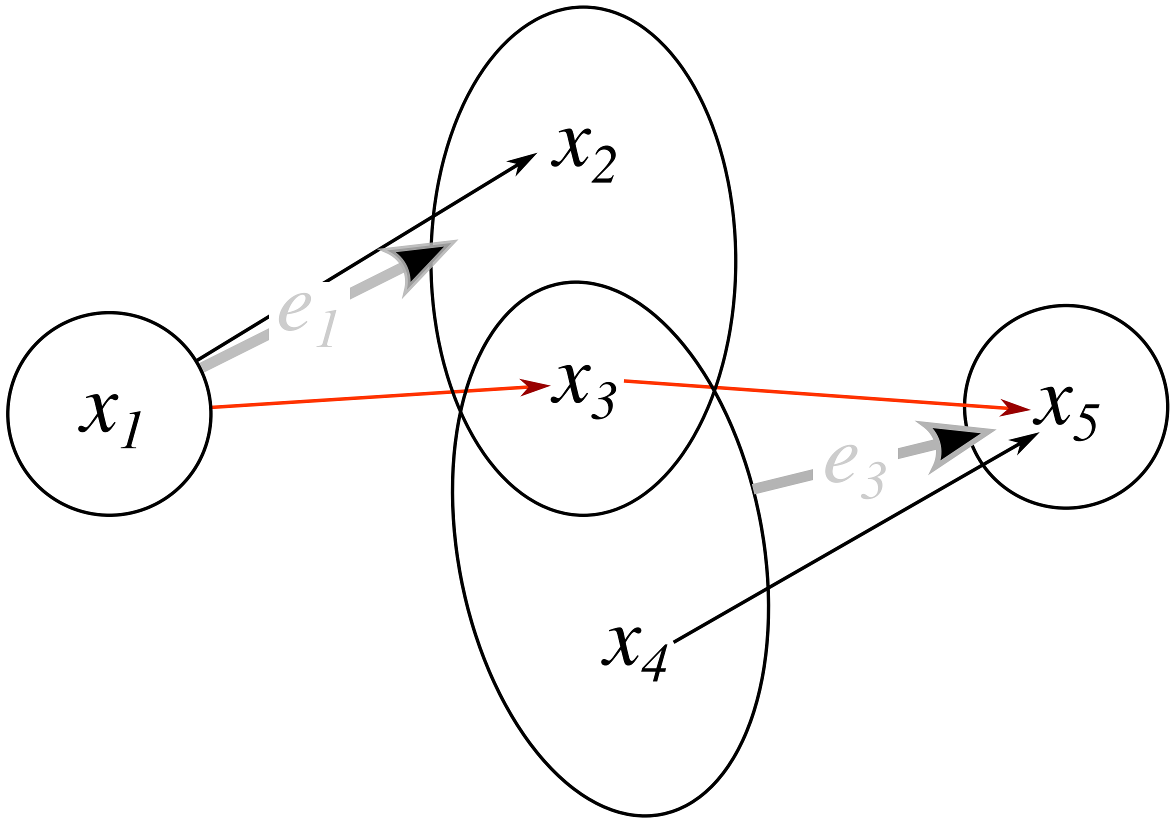
Paths in Metagraphs

Simple paths



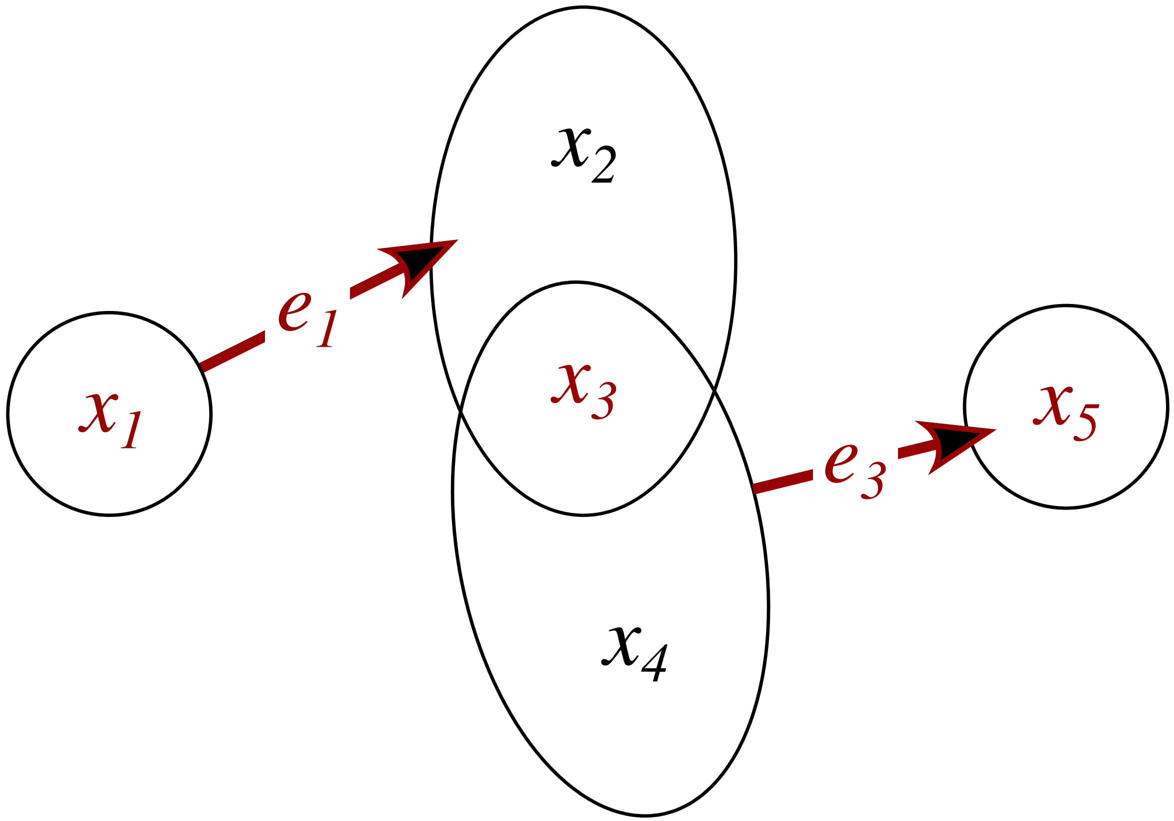
Paths in Metagraphs

Simple paths are just like expanding back to a full graph



Paths in Metagraphs

Simple paths lose information about groups

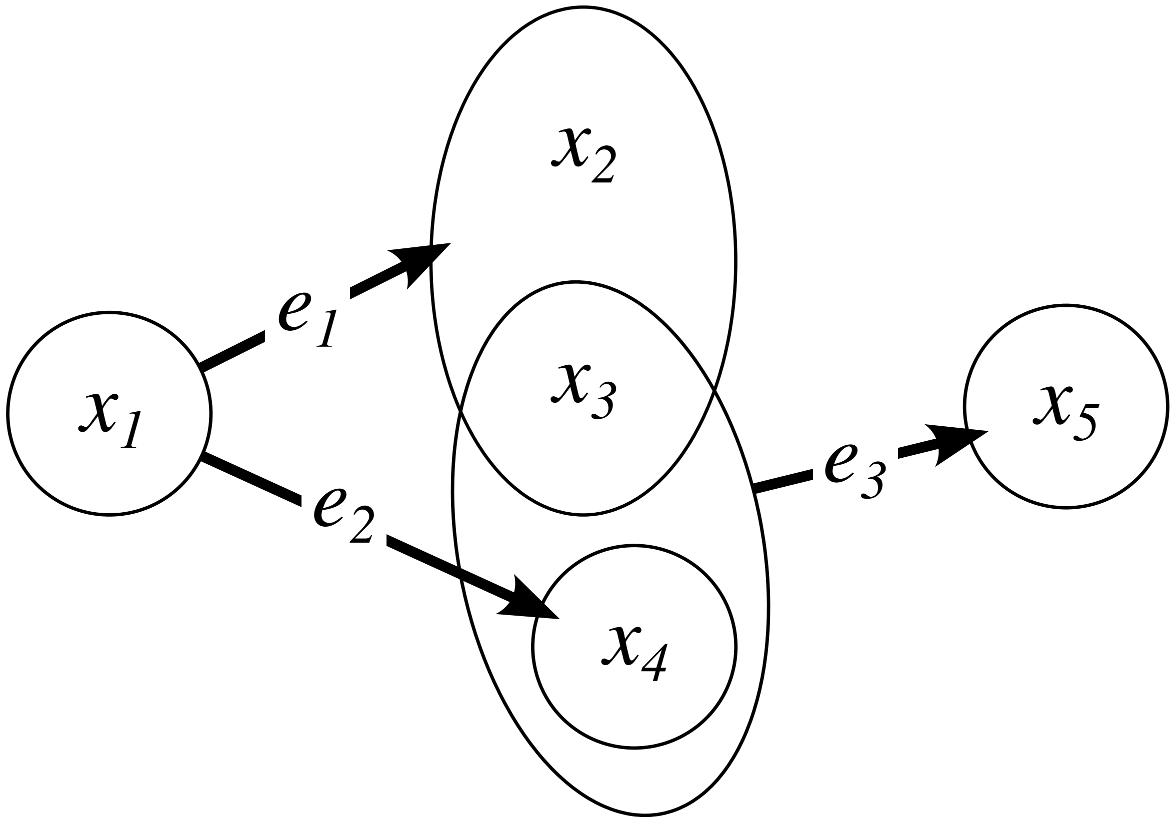


Metapaths (part 1)

Metapath

Think of the *in-set* as unlocking the *out-set*

The meta-edge e_3 means that $x_3\ AND\ x_4\ unlocks\ x_5$



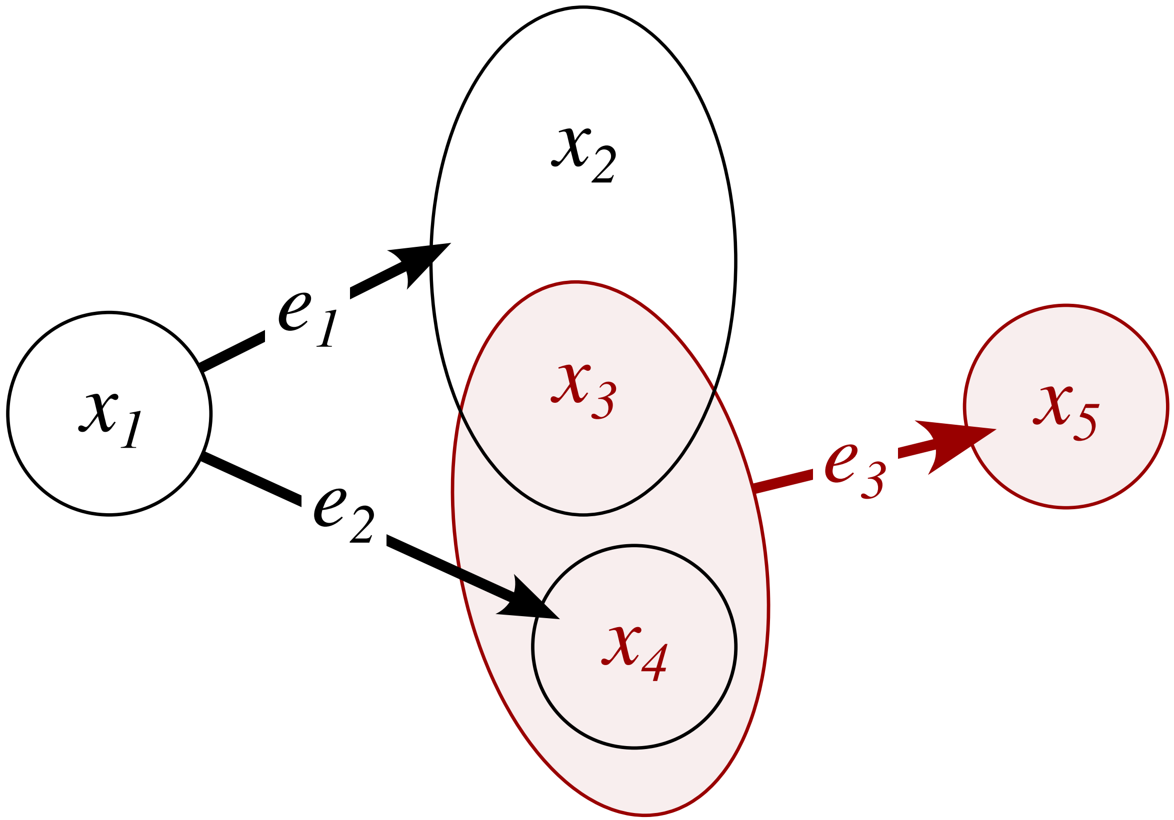
Unlocks == activates == depends on == …

Metapaths (part 1)

Metapath from

$$\boldsymbol{x_1 \to x_5}$$

Working backwards

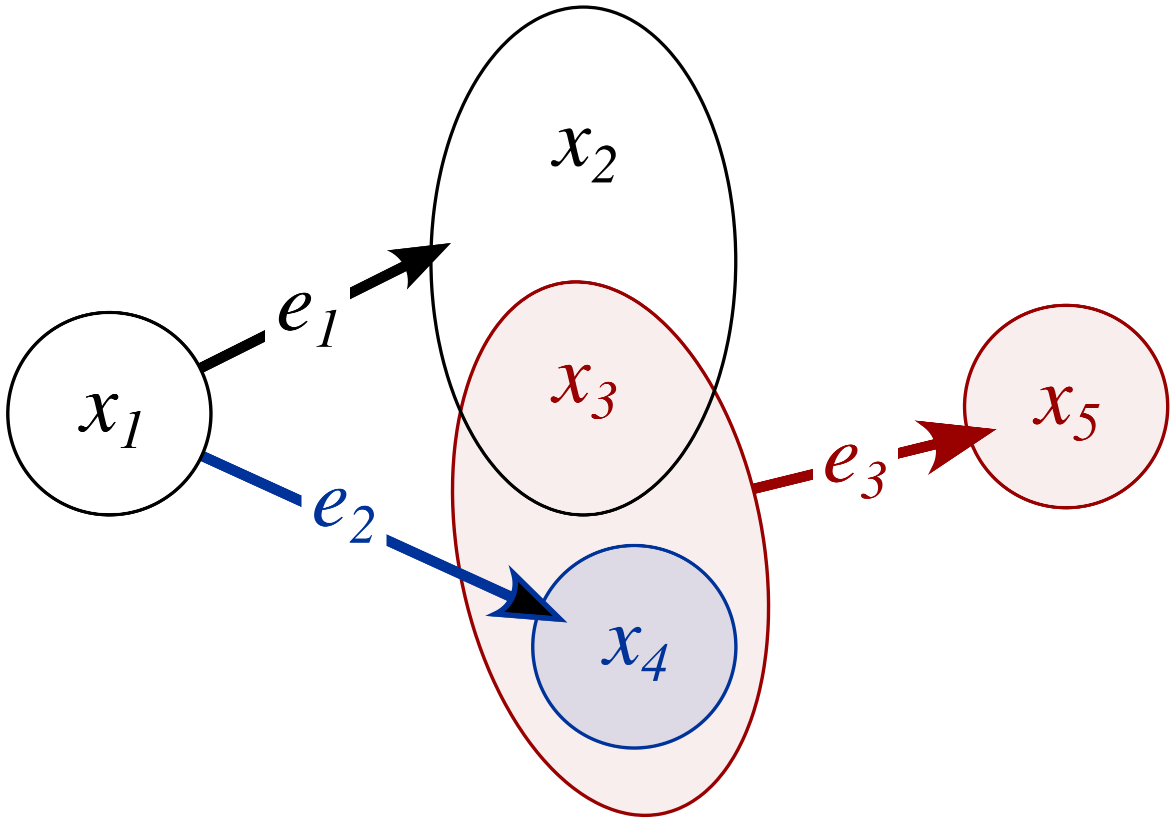


Metapaths (part 1)

Metapath from

$$\boldsymbol{x_1} \rightarrow \boldsymbol{x_5}$$

Working backwards

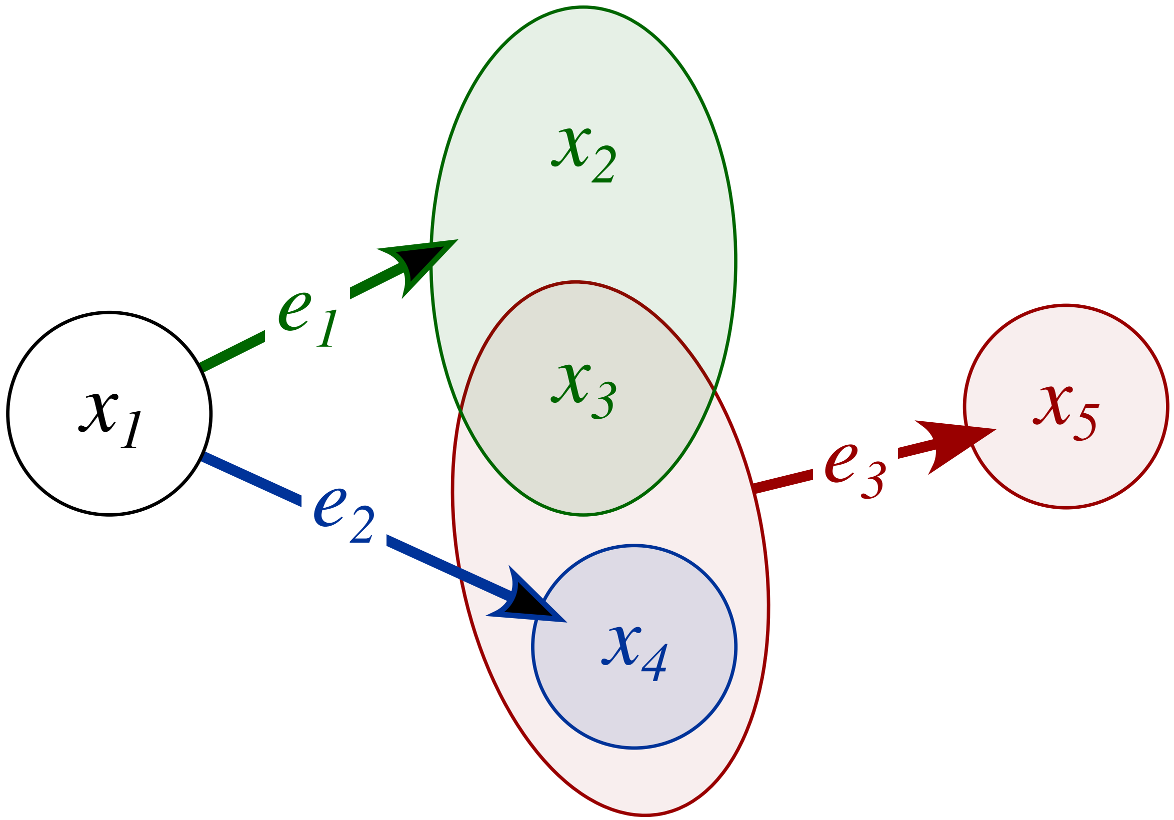


Metapaths (part 1)

Metapath from

$$\boldsymbol{x_1 \rightarrow x_5}$$

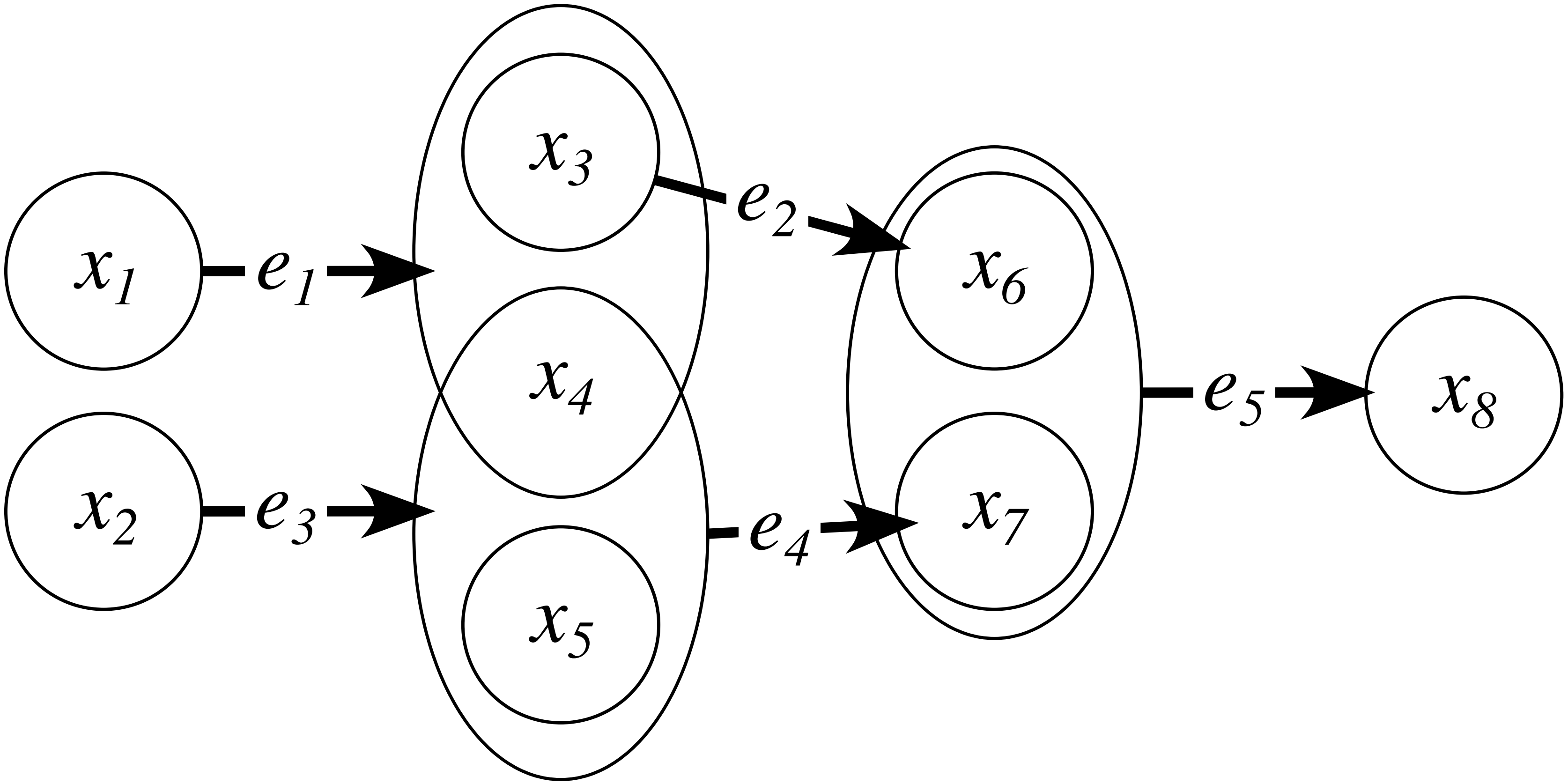
Working backwards



Metapaths (part 2)

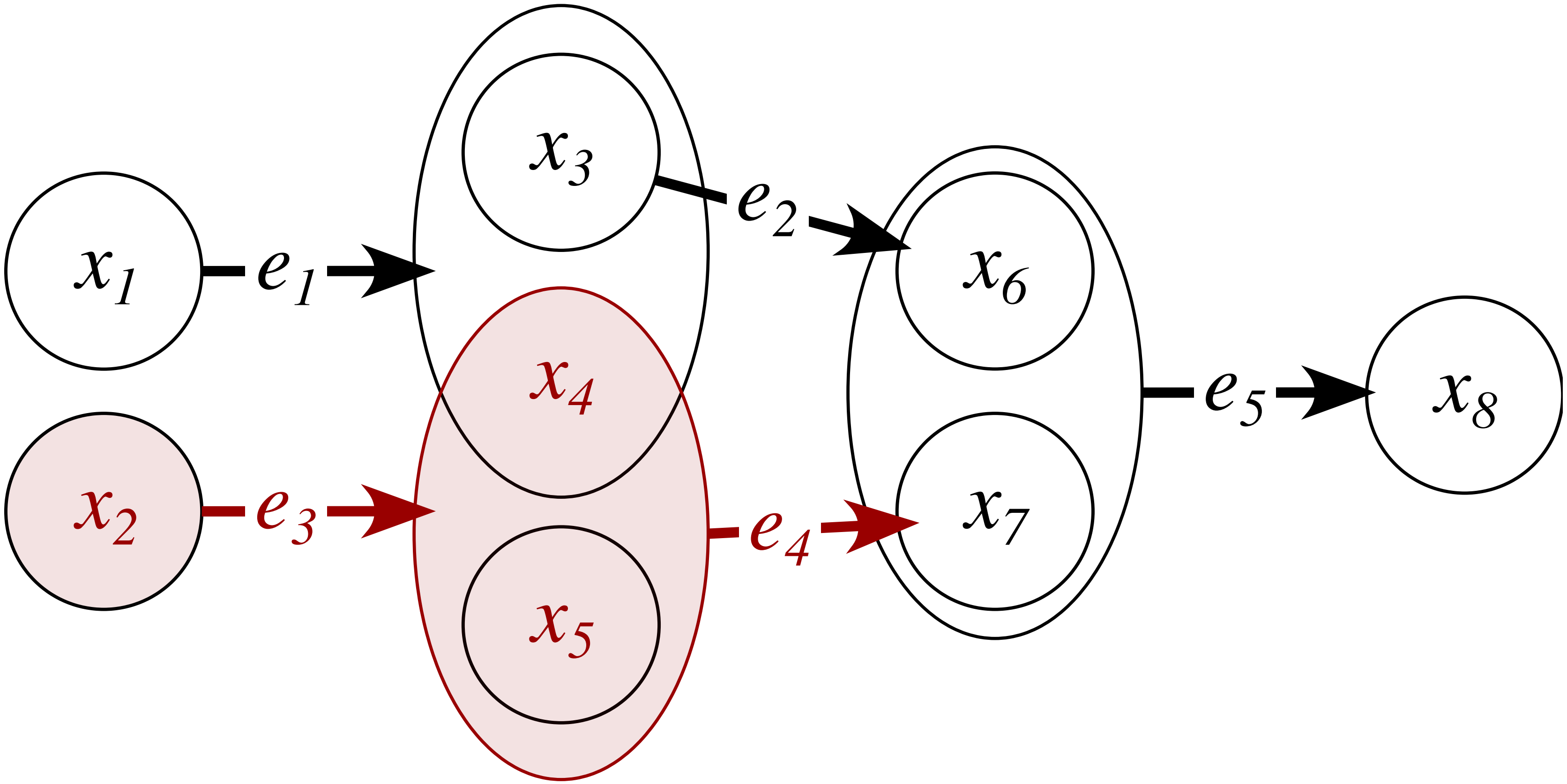
Metapath from $\{\boldsymbol{x_1}, \boldsymbol{x_2}\} \rightarrow \boldsymbol{x_7}$

Metapaths are between sets



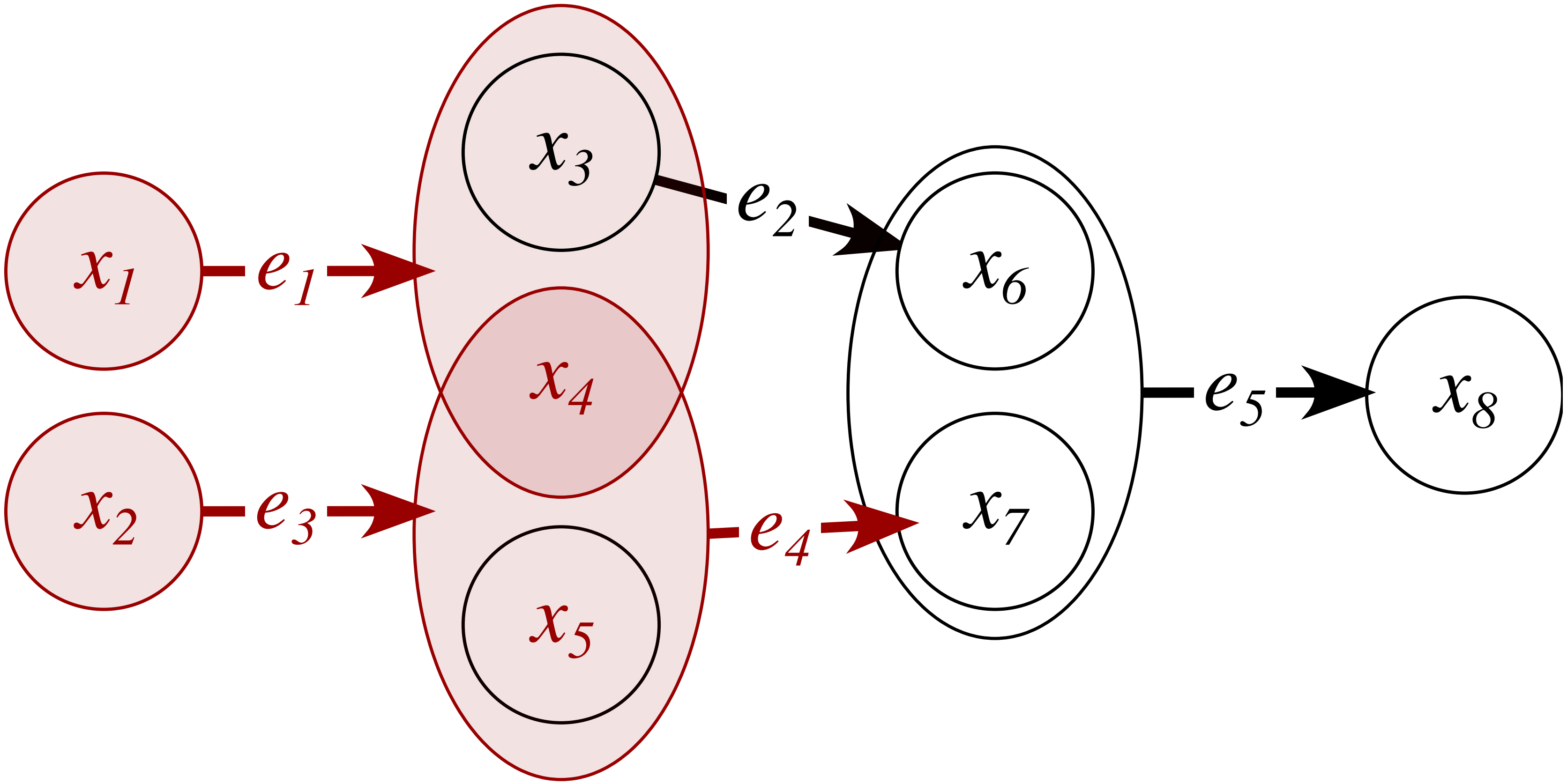
Metapaths (part 2)

Metapath from $\{x_1, x_2\} \rightarrow x_7$



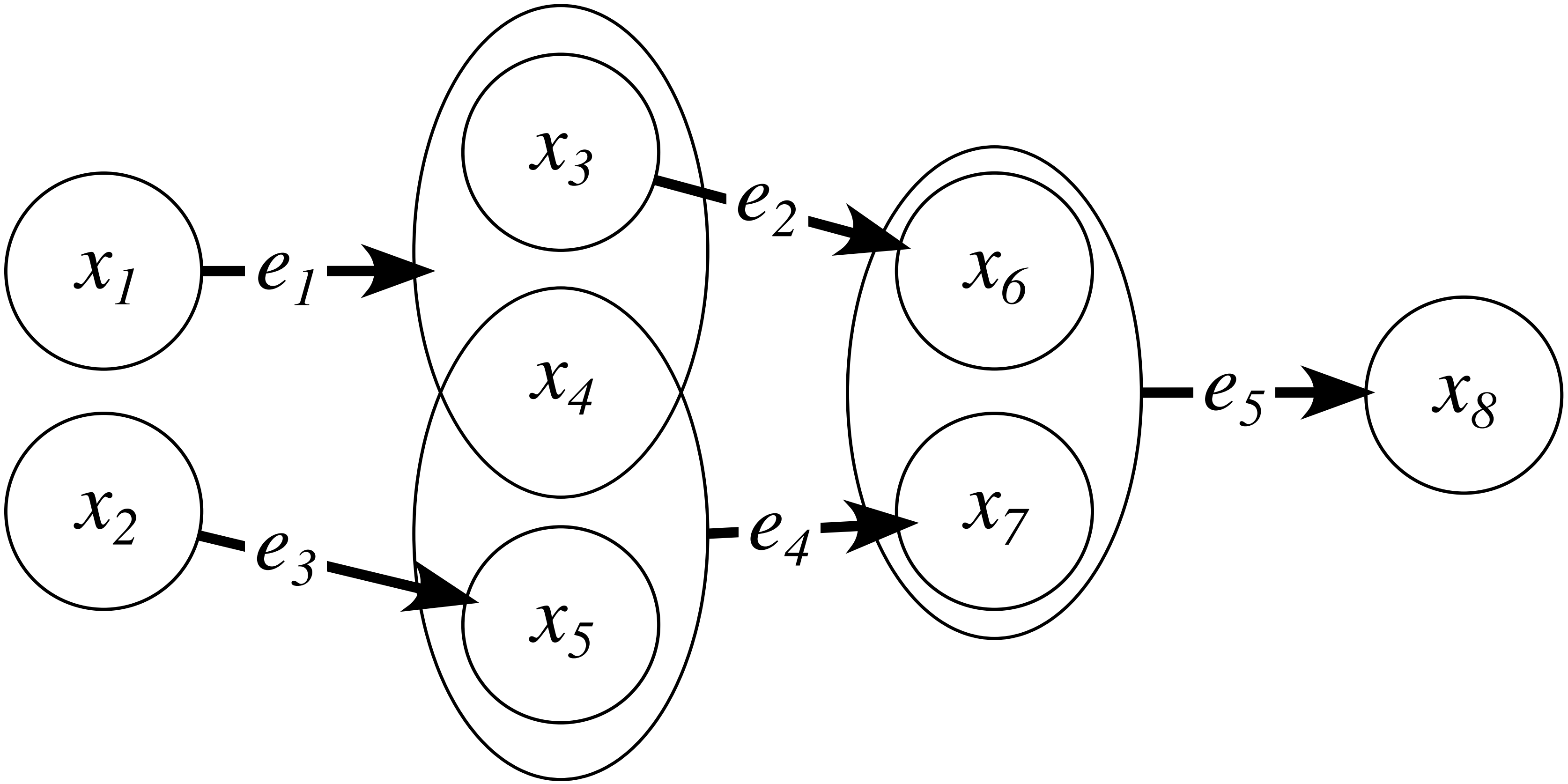
Metapaths (part 2)

Metapath from $\{x_1, x_2\} \rightarrow x_7$ but this one is non-dominant



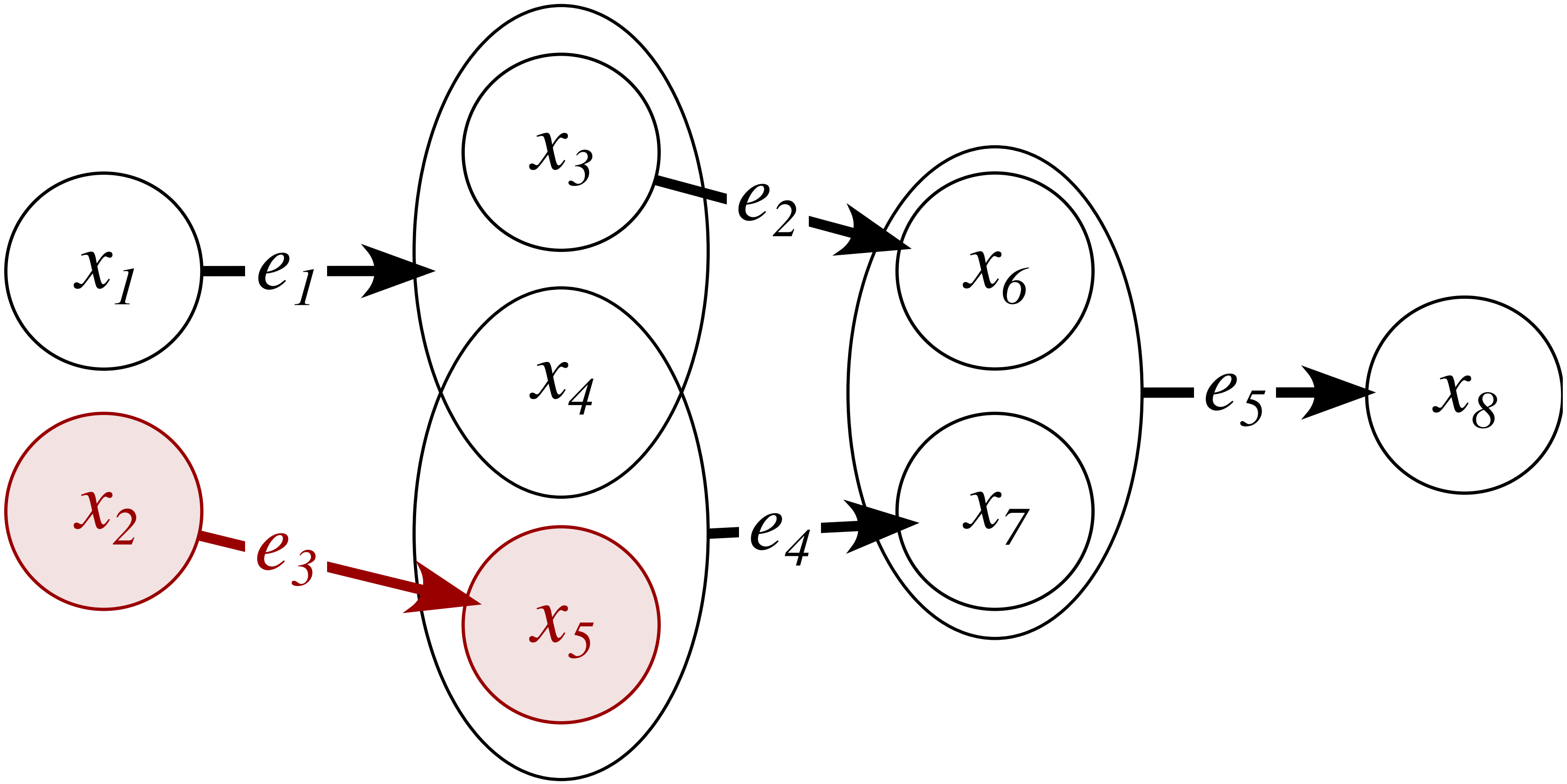
Metapaths (part 3)

Metapath from $\{\boldsymbol{x_1}, \boldsymbol{x_2}\} \rightarrow \boldsymbol{x_7}$



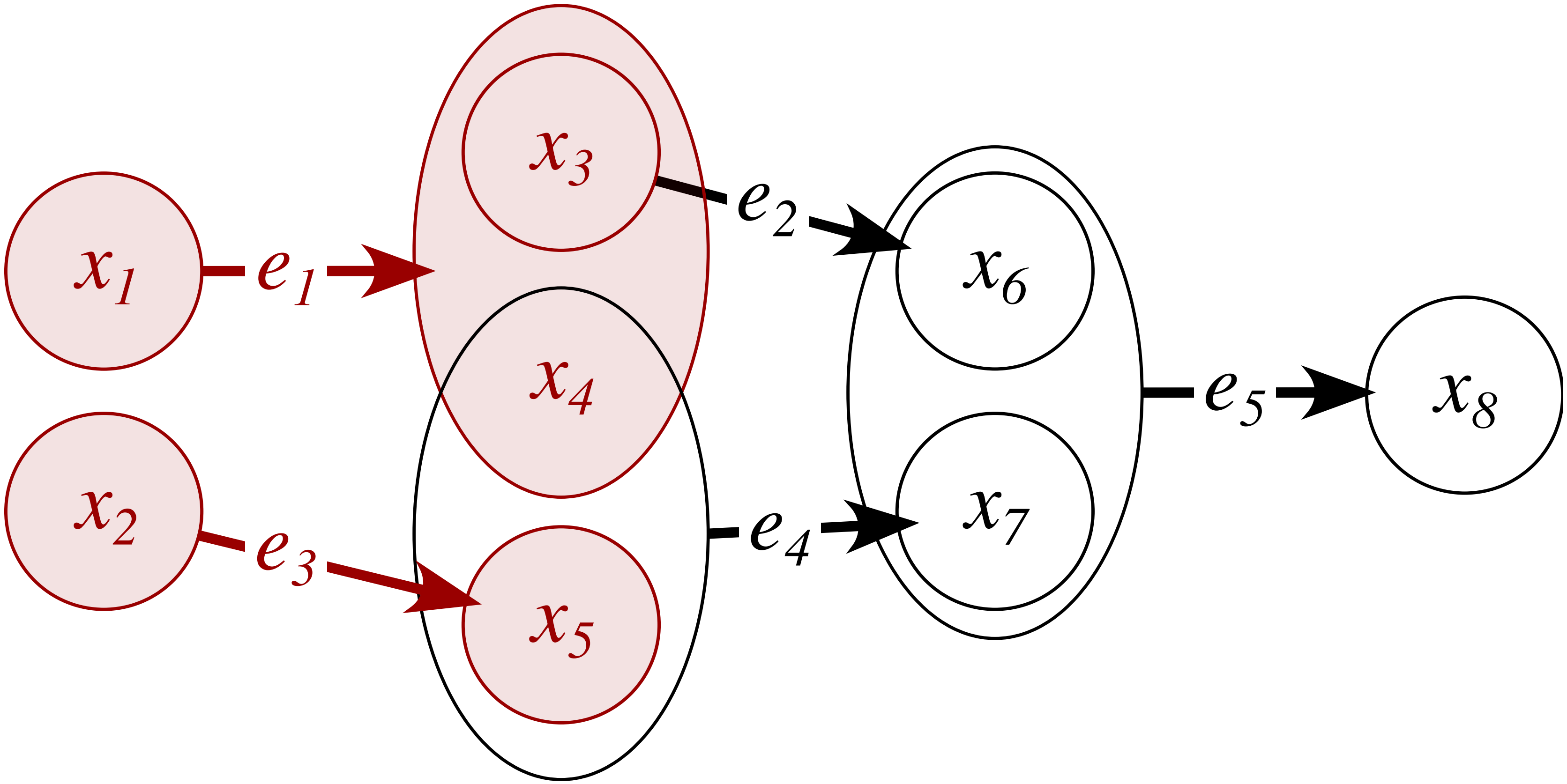
Metapaths (part 3)

Metapath from $\{x_1, x_2\} \rightarrow x_7$



Metapaths (part 3)

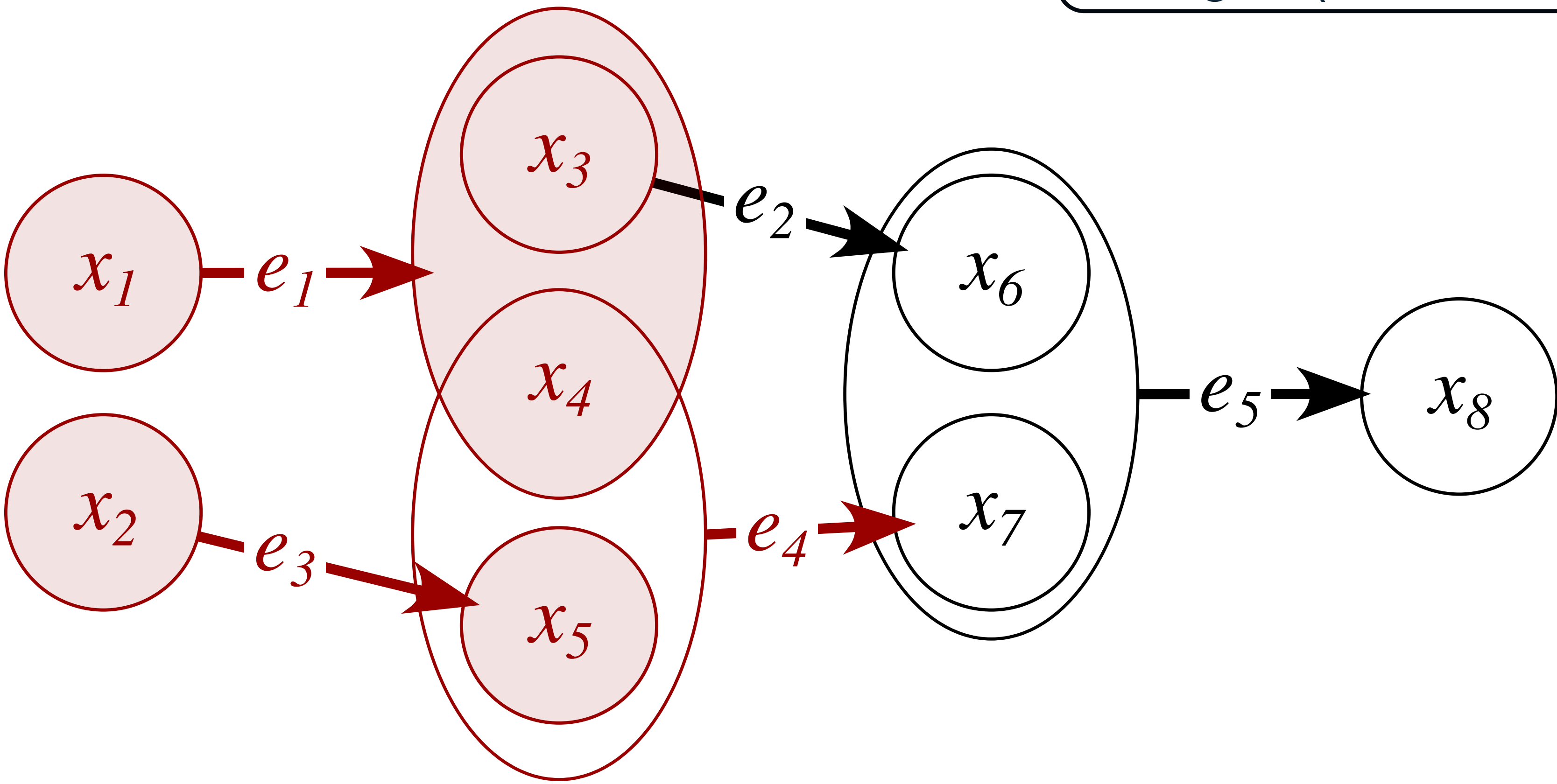
Metapath from $\{x_1, x_2\} \to x_7$



Metapaths (part 3)

Metapath from $\{x_1, x_2\} \rightarrow x_7$

A metapath is a set of edges (unordered)



Why Metapaths

Think of an edges as unlocking

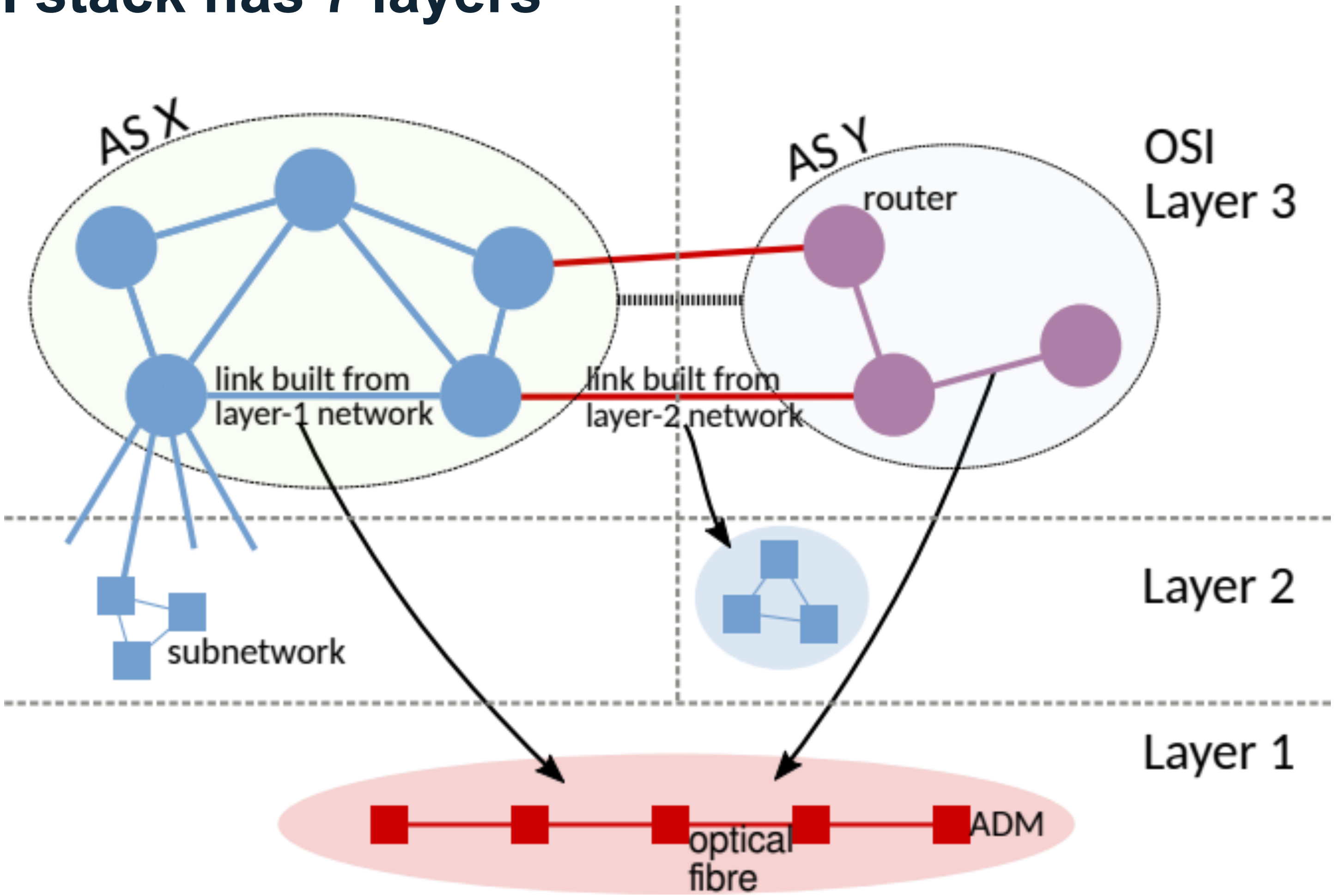
- Attacks
- Access to a resource or credential
- AND semantics

We can do more

- Add predicates (more meaning) to edges
- More algorithms and tools

Multilayered Networks

The OSI stack has 7 layers



But the Internet uses overlays

Multilayered Networks

Protocol Relationships – just thinking about names/addresses

DNS
maps URLs to
IP addresses

NAT
translates external
IP address to interna

DHCP
allocate IP
addresses

iRouting*
finds internal IP
address location

BGP
finds external IP
address location

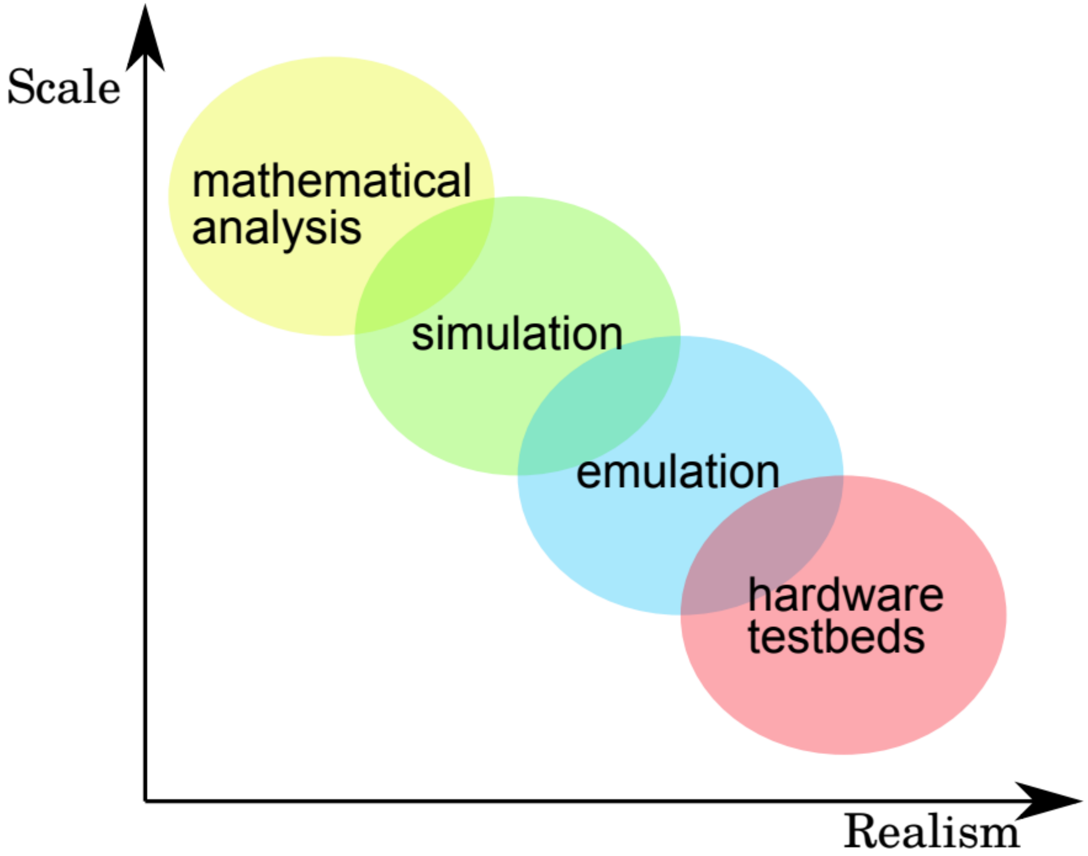
ARP
maps
IP address to
MAC address

Each of these distributed (in every way) and complex and a potential security vulnerability. They all interact, and run on top of, and support a vast set of other protocols

CORE – network emulation

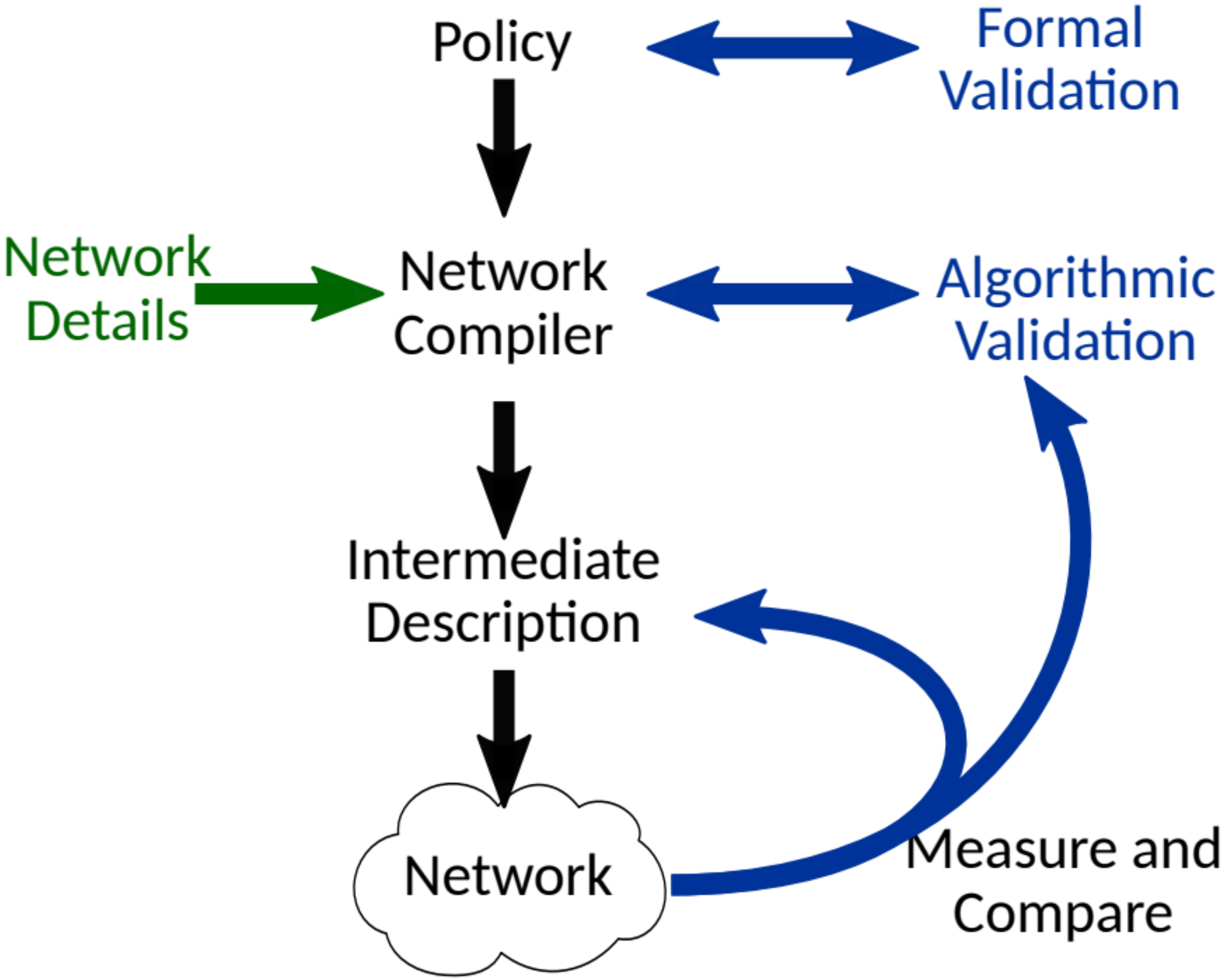
Common Open Research Emulator (CORE) lets you build real (but virtual) networks

1. Run real applications
   a. Web browsers, …
2. Connect hardware
3. But it's as much trouble to use as a real network



https://www.nrl.navy.mil/Our-Work/Areas-of-Research/Information-Technology/NCS/CORE/

Systems



Policy
Formal Validation
Network Details
Network Compiler
Algorithmic Validation
Intermediate Description
Network
Measure and Compare

mgtookit

Python to do metagraphs

- **Current version is being upgraded, more news soon**
- **Dot-like syntax for inputting metagraphs**
- **A set of algorithms**
  - **Not all we need**
  - **Not efficient enough yet**

Conclusion

We're not really finished yet!

I haven't talked about

- **Algorithms (path finding, projection, kernel graphs, …)**
- **Visualisation**
- **Algebras that live on top of graphs -- semirings**