34th IEEE Computer Security Foundations Symposium, 2021

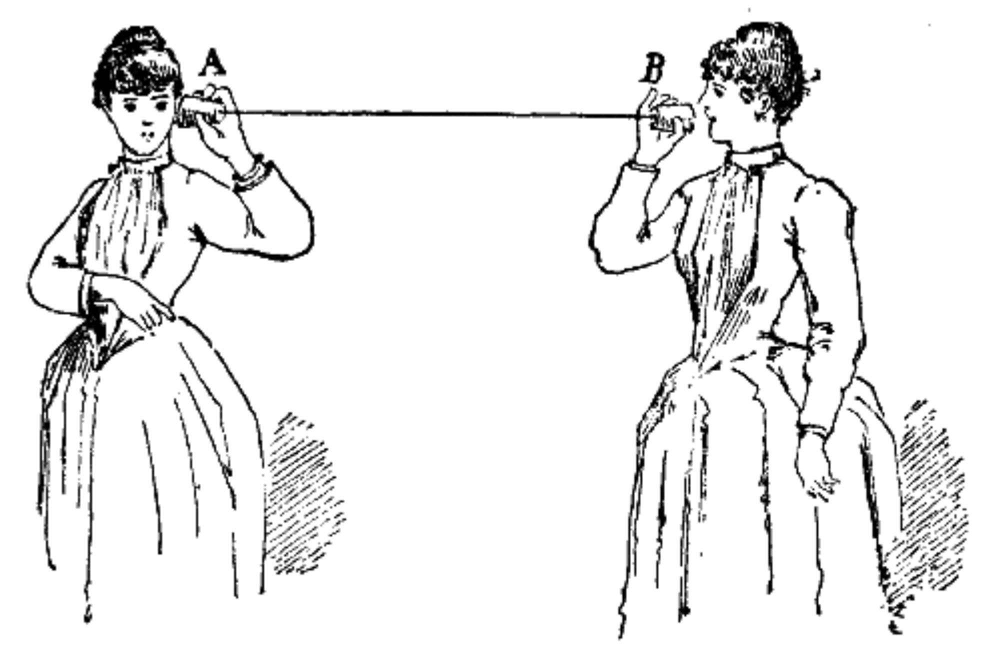
A Quantale of Information

Sebastian Hunt
City, U. London

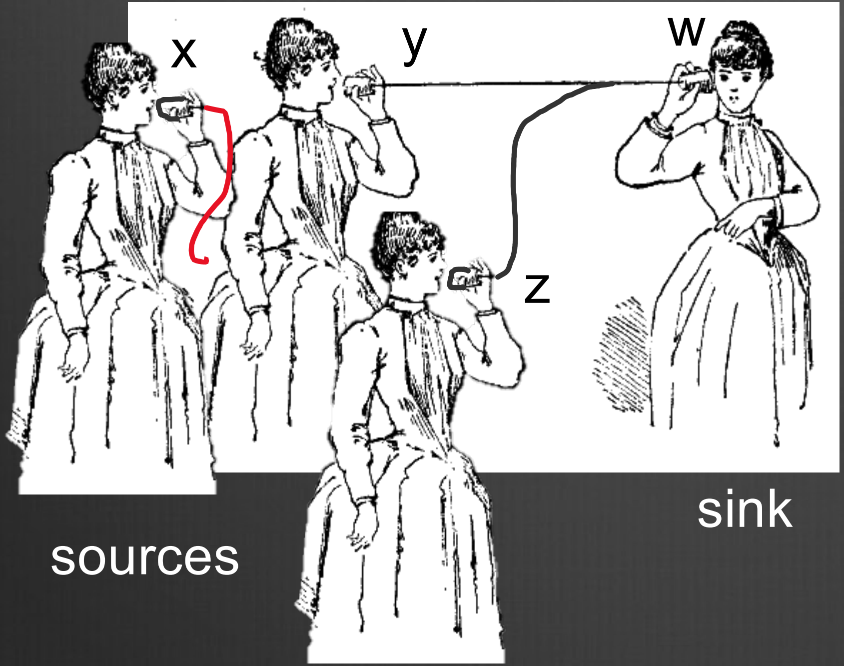
David Sands
Chalmers, SE

(speaker/ dave@chalmers.se)

Information Flow



= Dependency

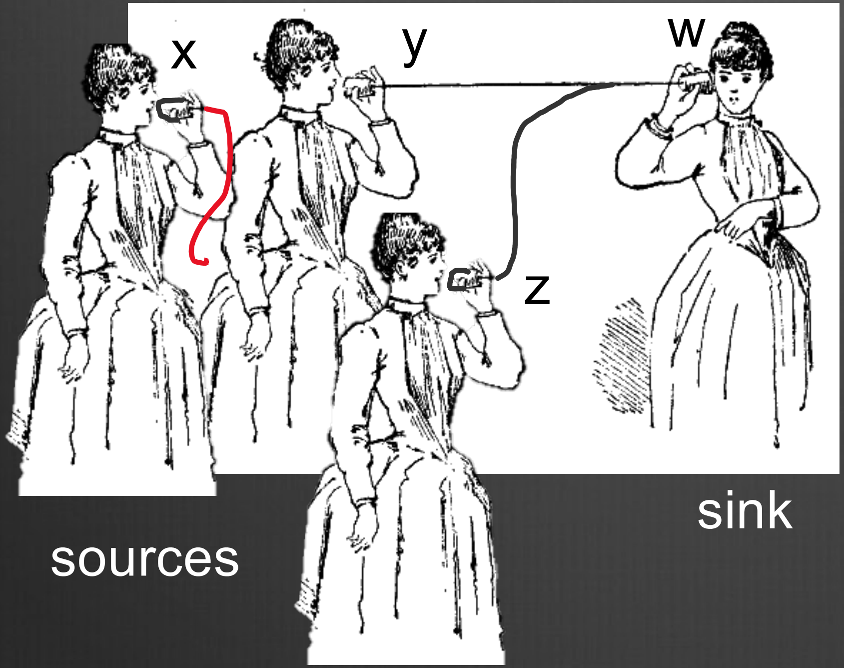


sources

sink

w depends on
y and z

Conjunctive Dependency

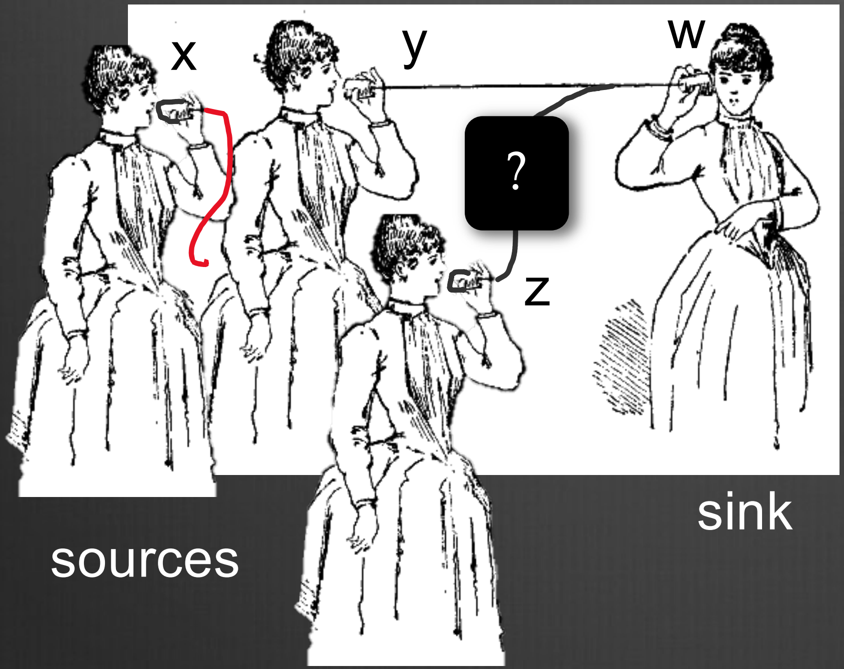


sources

sink

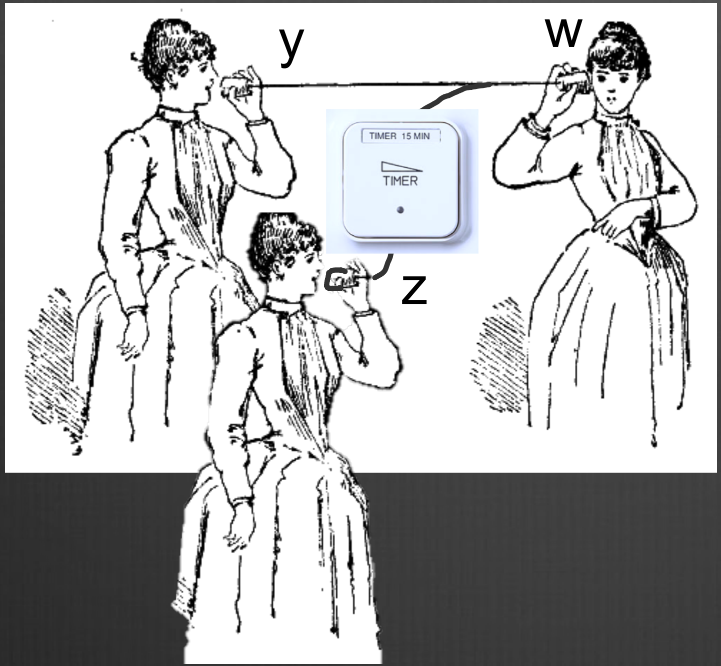
w depends on
y and z

Conjunctive Dependency



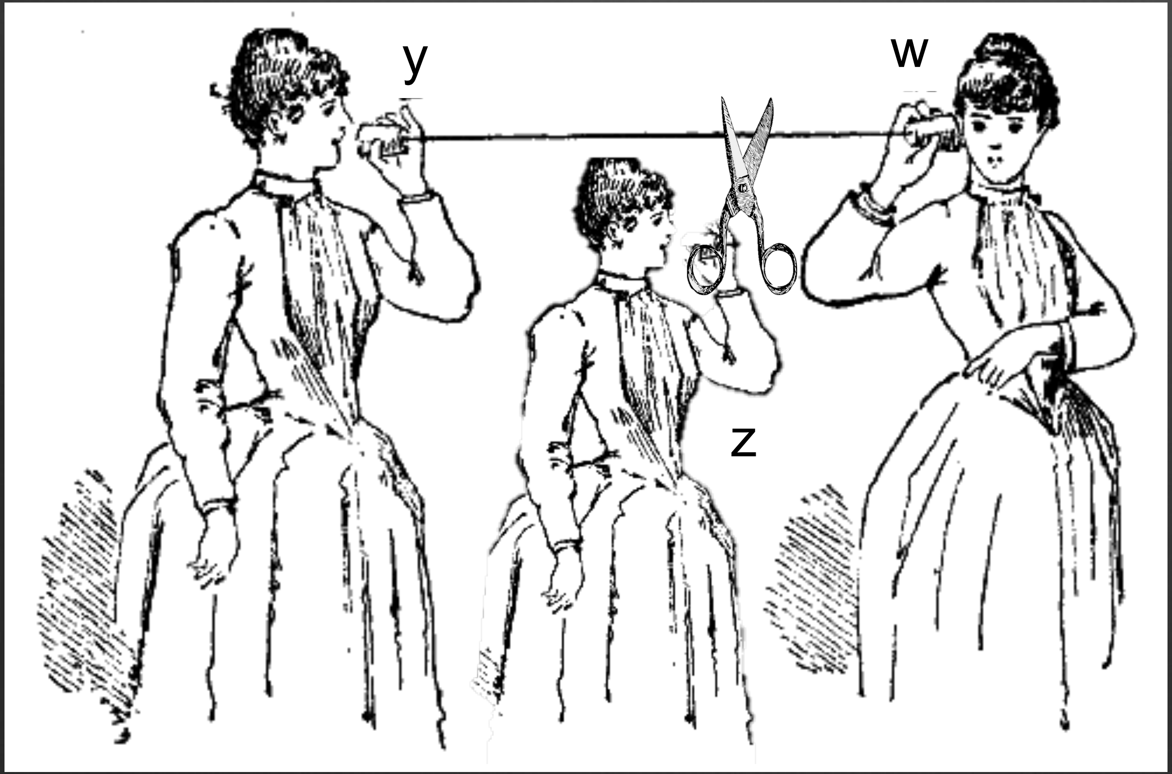
w depends on
y and z

Fine-Grained Dependency



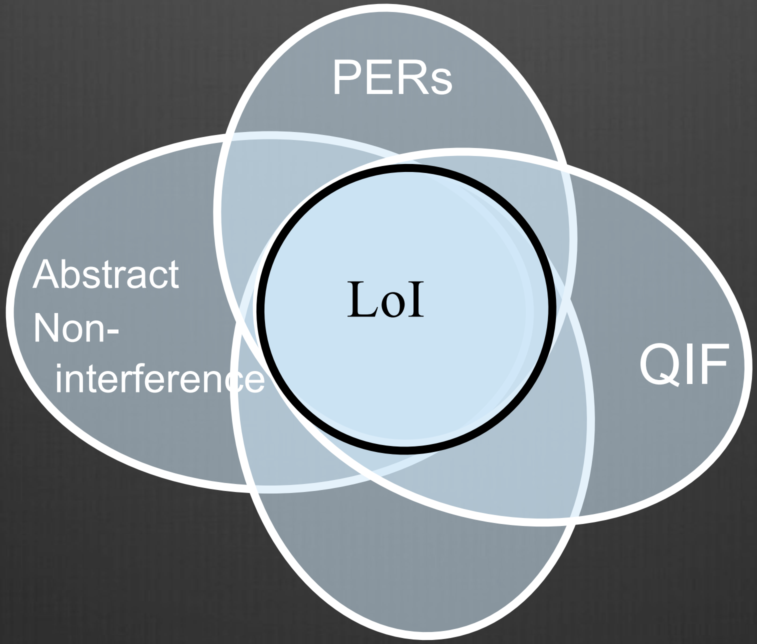
w depends on
y and the first 5
minutes of z

Conditional Dependency

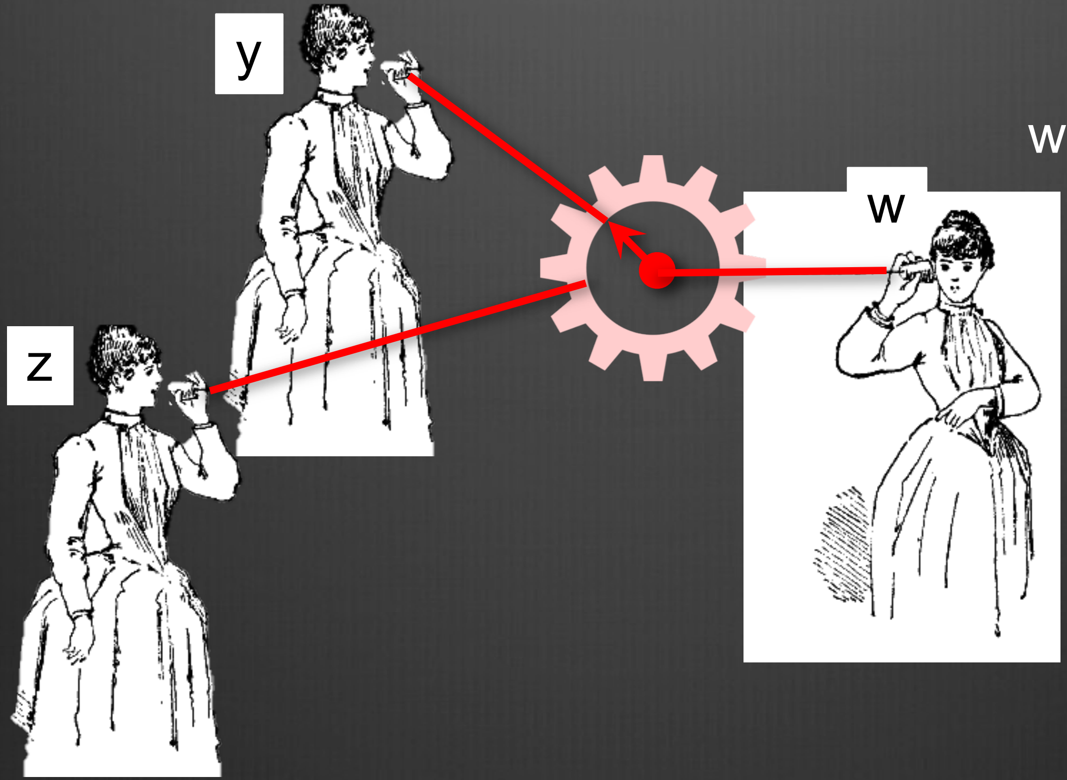


The Lattice of Information

Various semantic models of information flow use equivalence relations to model information



A missing abstraction:
disjunctive information flow



w depends on

y or z

Disjunctive Information Flow

$$\text{if } x \text{ then } w = y \text{ else } w = z \quad \left\{ \begin{array}{c} \text{w depends on} \\ \text{x and y} \\ \text{or} \\ \text{x and z} \end{array} \right.$$

Disjunctive Information Flow
What is it Good For?

Brewer & Nash
IEEE Securty & Privacy 1989

THE CHINESE WALL SECURITY POLICY

Dr. David F.C. Brewer and Dr. Michael J. Nash

GAMMA SECURE SYSTEMS LIMITED
9 Glenhurst Close, Blackwater, Camberley, Surrey, GU17 9BQ, United Kingdom

ABSTRACT

Everyone who has seen the movie Wall Street will have seen a commercial security policy in action. The recent work of Clark and Wilson and the WIPCIS initiative (the Workshop on Integrity Policy for Computer Information Systems) has drawn attention to the existence of a wide range of commercial security policies which are both significantly different from each other and quite alien to current "military" thinking as implemented in products for the security market place.

This paper presents a basic mathematical theory which implements one such policy, the Chinese Wall, and shows that it cannot be correctly represented by a Bell-LaPadula model.

The Chinese Wall policy combines commercial discretion with legally enforceable mandatory controls. It is required in the operation of many financial services organizations and is, therefore, perhaps as significant to the financial world as Bell-LaPadula's policies are to the military.

INTRODUCTION

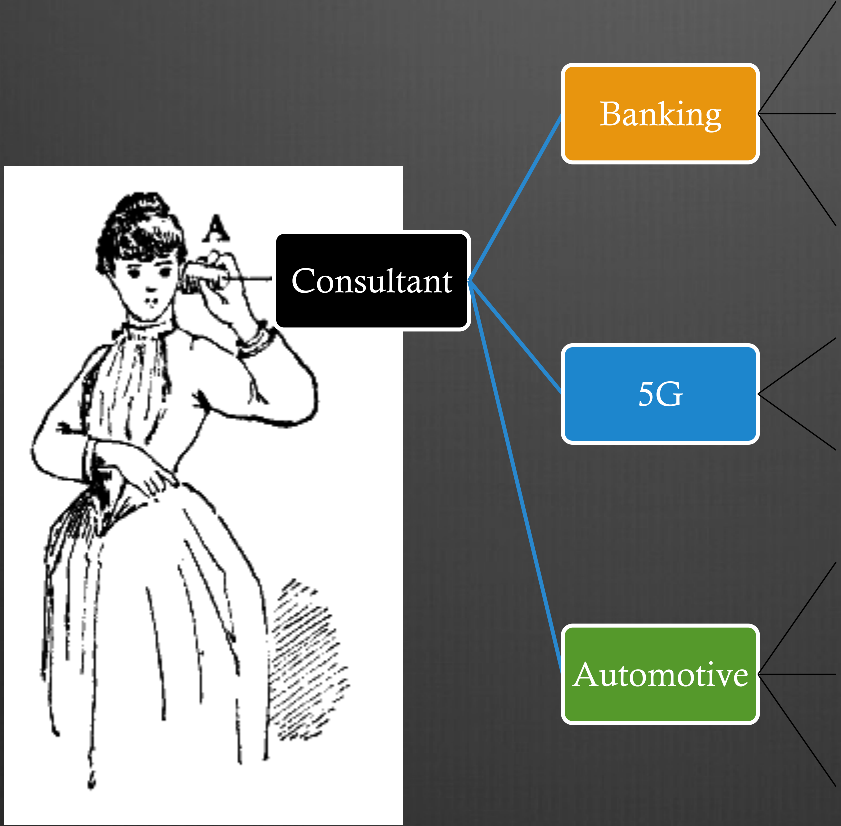
Until recently, military security policy thinking has

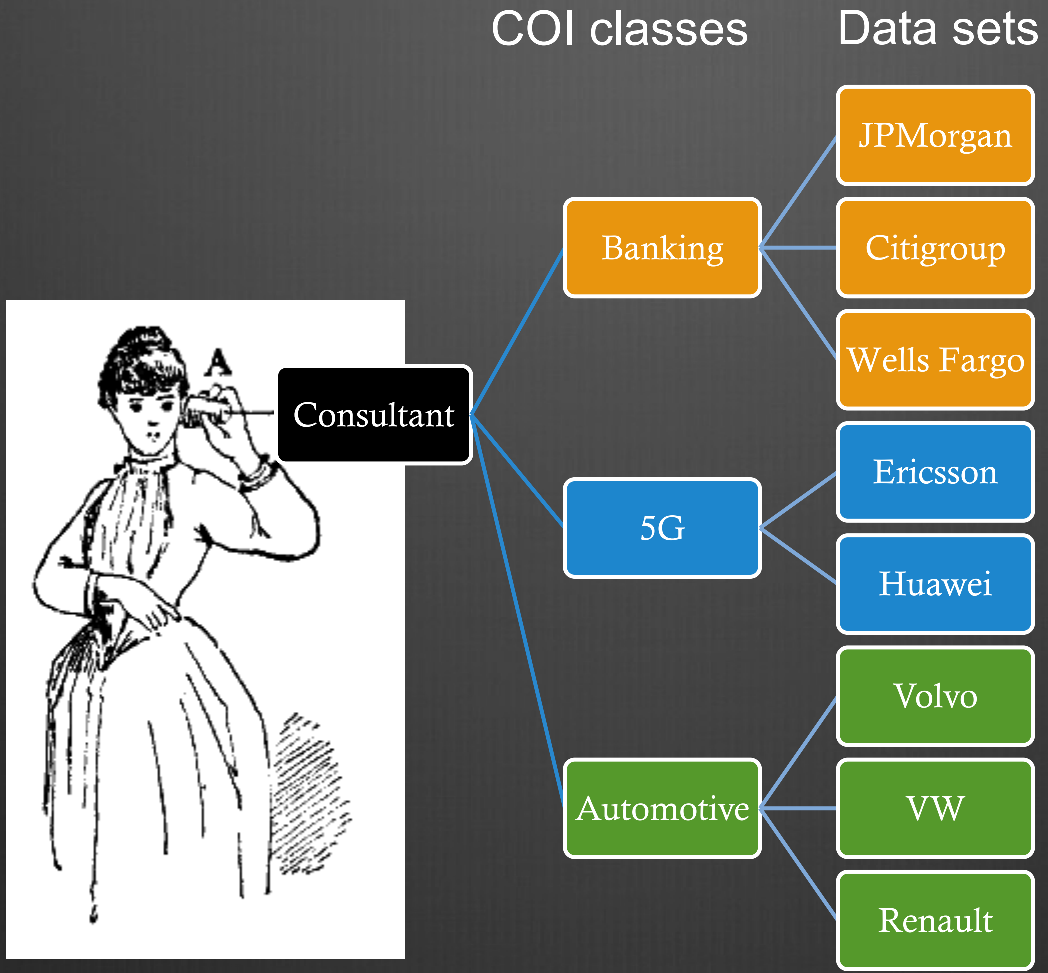
However, the analyst is free to advise corporations which are not in competition with each other, and also to draw on general market information. Many other instances of Chinese Walls are found in the financial world.

Unlike Bell and LaPadula, access to data is not constrained by attributes of the data in question but by what data the subject already holds access rights to. Essentially, datasets are grouped into "conflict of interest classes" and by mandatory ruling all subjects are allowed access to at most one dataset belonging to each such conflict of interest class; the actual choice of dataset is totally unrestrained provided that this mandatory rule is satisfied. We assert that such policies cannot be correctly modelled by Bell-LaPadula.

It should be noted that in the United Kingdom the Chinese Wall requirements of the UK Stock Exchange [6] have the authority of law [7] and thus represent a mandatory security policy whether implemented by manual or automated means.

Furthermore, correct implementation of this policy is important to English Financial Institutions since it provides a legitimate defence against certain penal classes of offence under their law.


A
Consultant
Banking
5G
Automotive


COI classes
Data sets
A
Consultant
Banking
5G
Automotive
JPMorgan
Citigroup
Wells Fargo
Ericsson
Huawei
Volvo
VW
Renault

Contributions

A semantic model for disjunctive information flow generalising the lattice of information

- Disjunctive policies (ethical wall)

Model enjoys properties useful for reasoning about programs

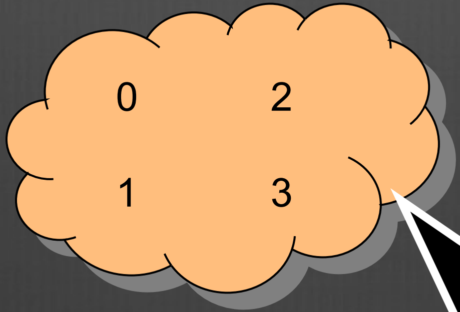
- Disjunctive completion of IF lattices
- Compositional reasoning principles

The Lattice of Information

Equivalence Relations as Partitions

Assume (e.g.) a data domain D = {0,…,3}

We assume that the observer knows the data domain itself

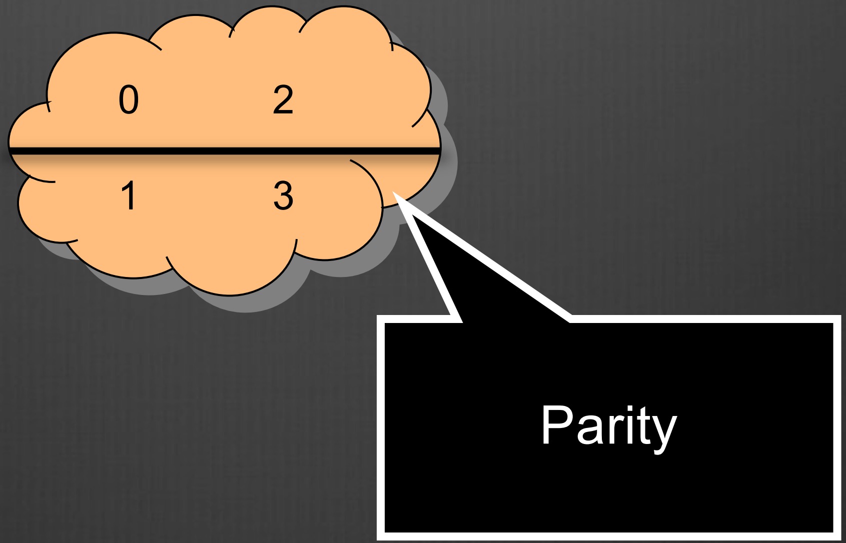


zero partitions = zero knowledge

Equivalence Relations as Partitions

Assume (e.g.) a data domain D = {0,…,3}

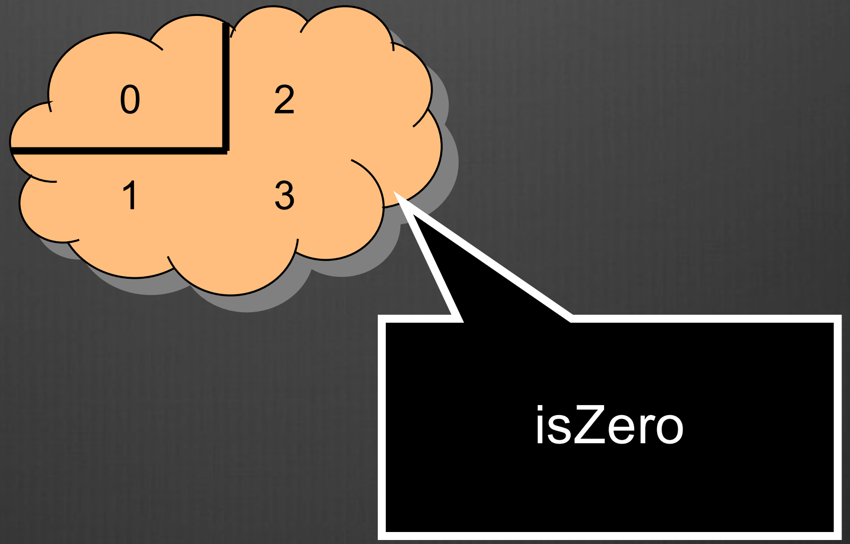
output (d div 2)



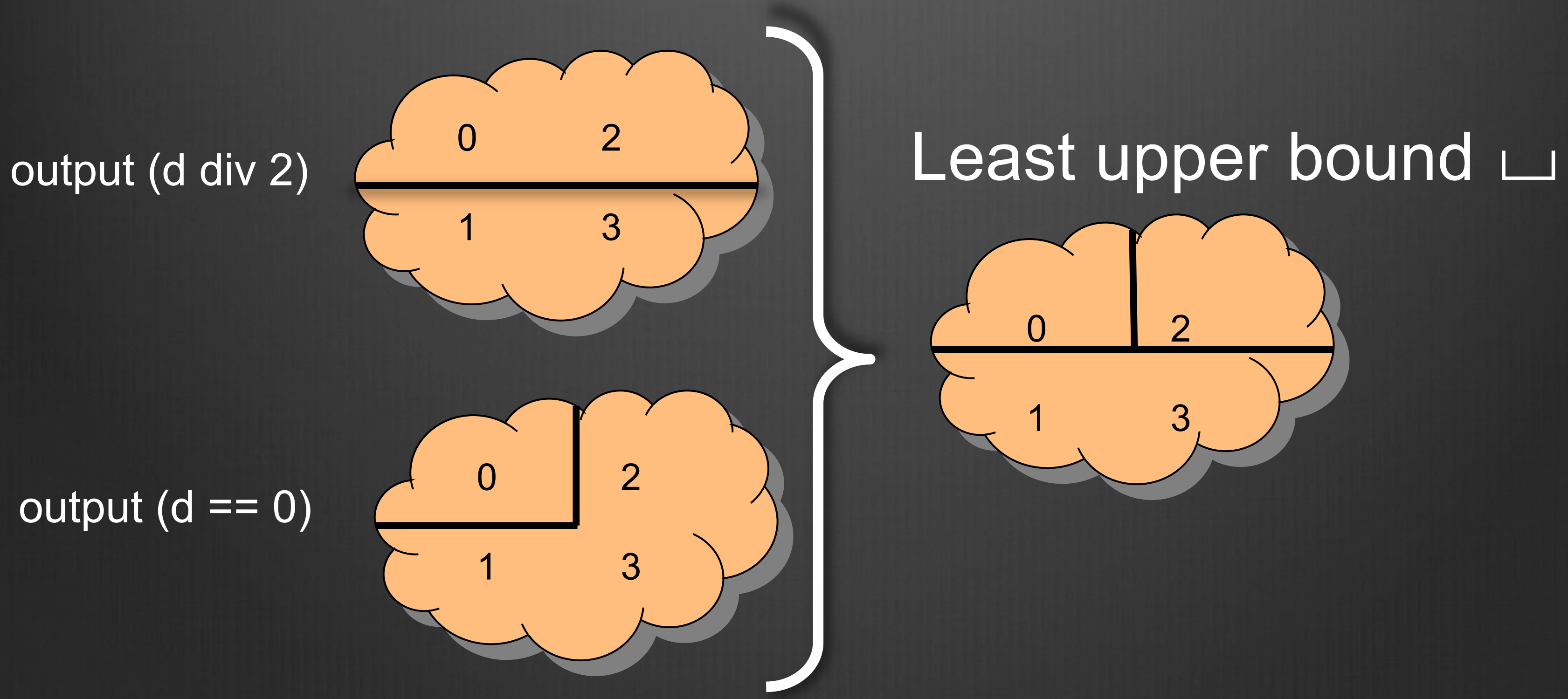
Equivalence Relations as Partitions

Assume (e.g.) a data domain D = {0,…,3}

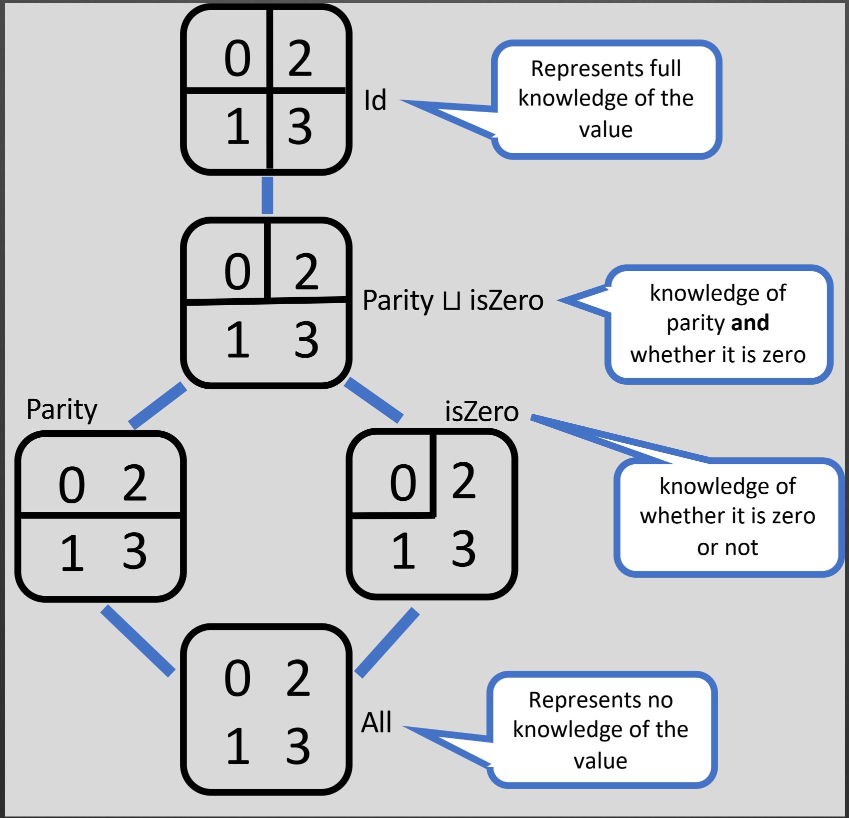
output (d == 0)



The Lattice of Partitions

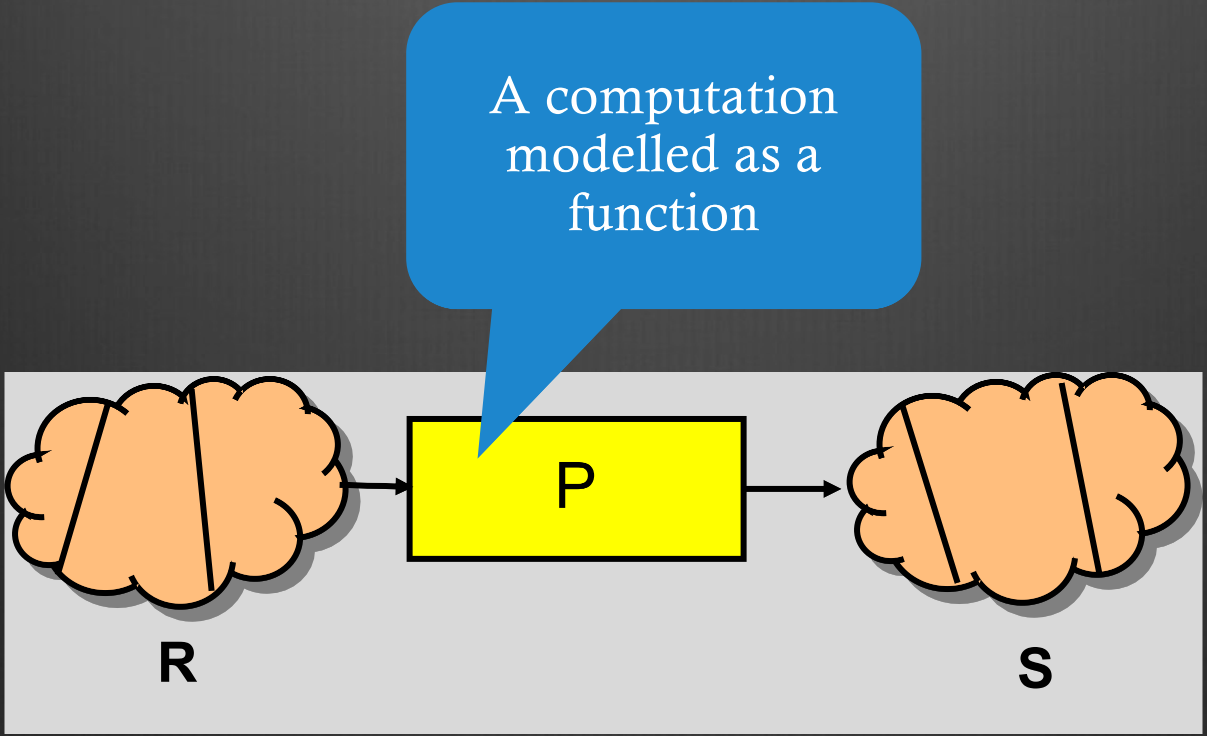


The lattice of Information

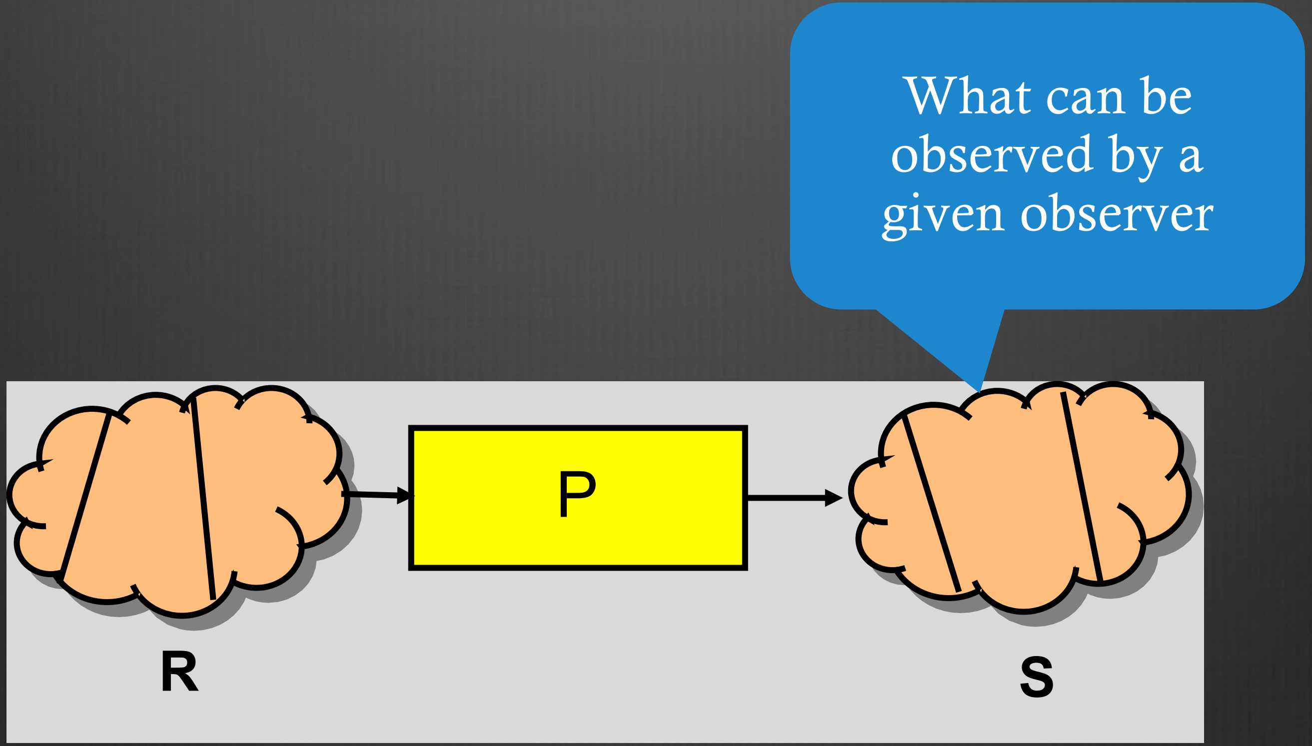


A sublattice of LoI(D)

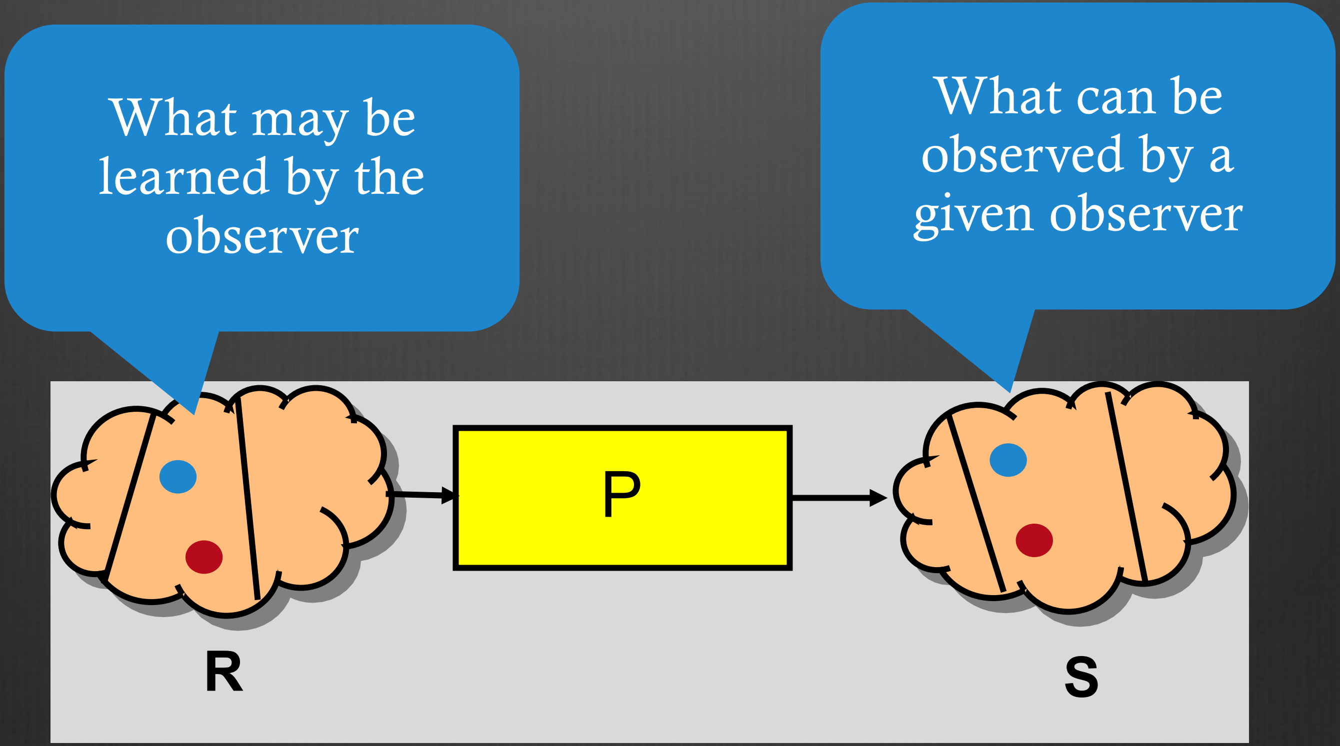
Information Flow Properties



Information Flow Properties



Information Flow Properties

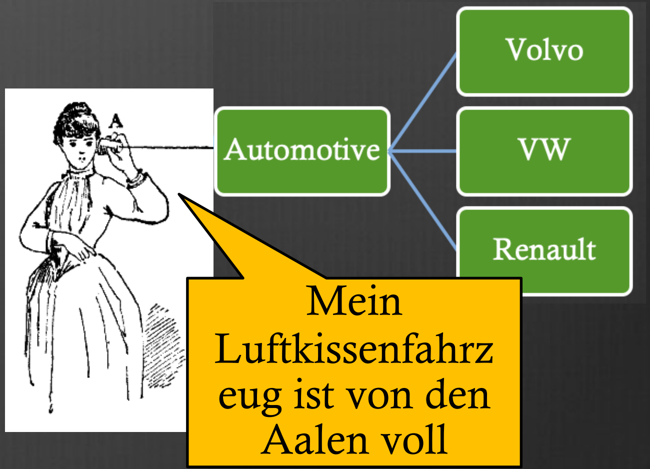


"P maps R-equivalent things to S-equivalent things"

Expressing disjunctive policies?

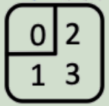
LoI can express a *specific* instance of a disjunctive flow:

"VW data flows to Consultant if they speak German, otherwise Volvo data flows to consultant"

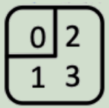
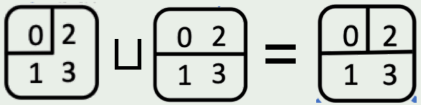


But such conditions may be complex, unknown, or irrelevant

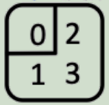
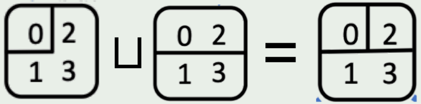
Lattice of Information

	Lattice of Information
Elements	Equivalence relations 
Conjunction of information	
Disjunctive of information	

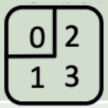
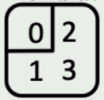
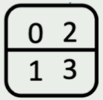
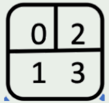
Lattice of Information

	Lattice of Information
Elements	Equivalence relations 
Conjunction of information	Lattice least upper bound ⊔ 
Disjunctive of information	

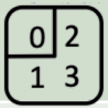
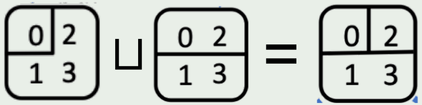
Lattice of Information

	Lattice of Information
Elements	Equivalence relations 
Conjunction of information	Lattice least upper bound ⊔ 
Disjunctive of information	✗

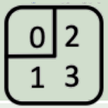
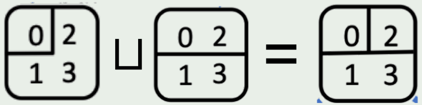
Quantale of Information

	Lattice of Information	Quantale of Information
Elements	Equivalence relations 	
Conjunction of information	Lattice least upper bound ⊔  ⊔  = 	
Disjunctive of information		

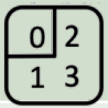
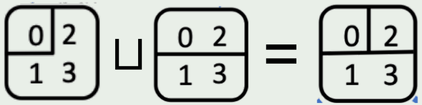
Quantale of Information

	Lattice of Information	**Quantale of Information**
Elements	Equivalence relations 	Sets of Equivalence relations
Conjunction of information	Lattice least upper bound ⊔ 	
Disjunctive of information		

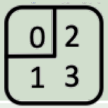
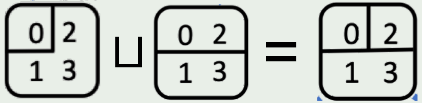
Quantale of Information

	Lattice of Information	Quantale of Information
Elements	Equivalence relations 	Sets of Equivalence relations
Conjunction of information	Lattice least upper bound ⊔ 	Tensor operator $\otimes$ $P \otimes Q = \{ p \sqcup q \mid p \in P, q \in Q \}$
Disjunctive of information		

Quantale of Information

	Lattice of Information	**Quantale of Information**
Elements	Equivalence relations 	Sets of Equivalence relations
Conjunction of information	Lattice least upper bound $\sqcup$ 	Tensor operator $\otimes$ $P \otimes Q = \{ p \sqcup q \mid p \in P, q \in Q \}$
Disjunctive of information		Lattice least upper bound = set union

Quantale of Information

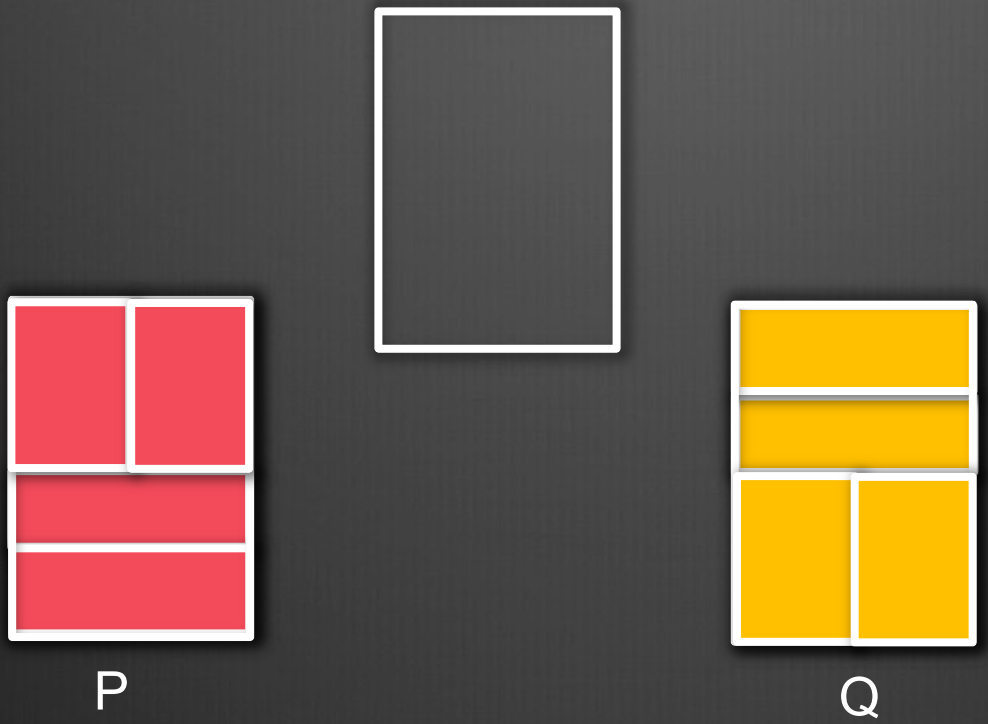
	Lattice of Information	Quantale of Information
Elements	Equivalence relations 	Sets of Equivalence relations (*)
Conjunction of information	Lattice least upper bound ⊔ 	Tensor operator $\otimes$ $P \otimes Q = \{\, p \sqcup q \mid p \in P,\ q \in Q \,\}$(*)
Disjunctive of information		Lattice least upper bound = set union (*)

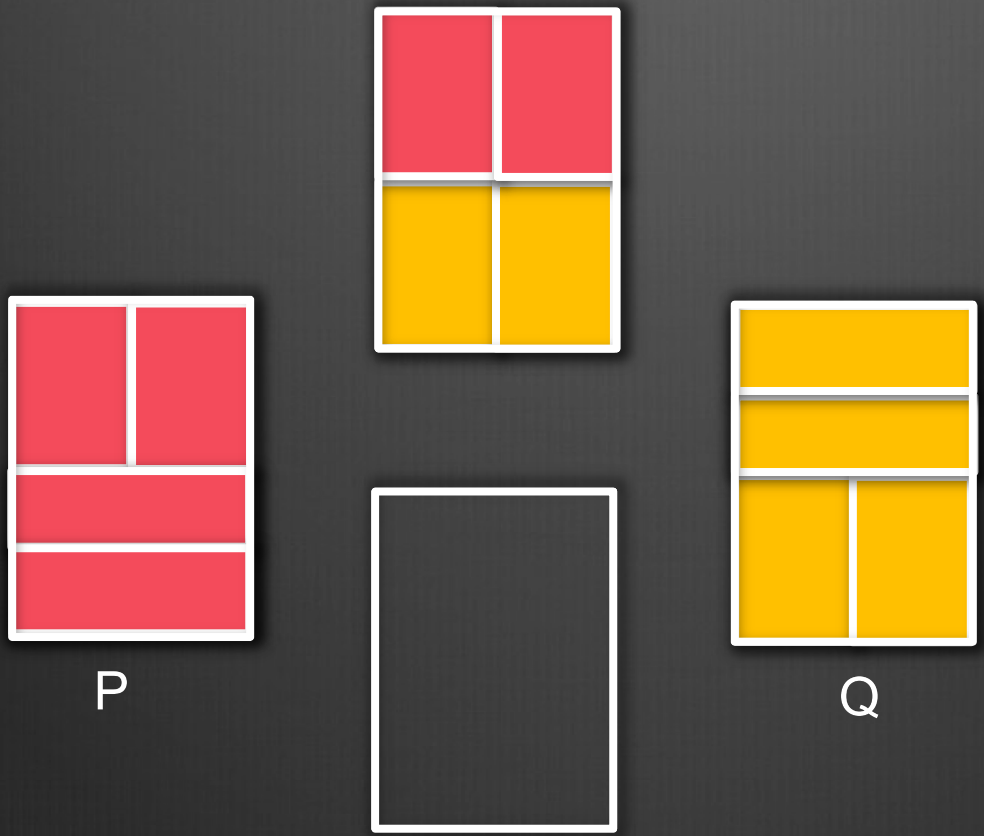
(*) Sets closed under a special "mixing" operations on sets of equivalence relations called tiling

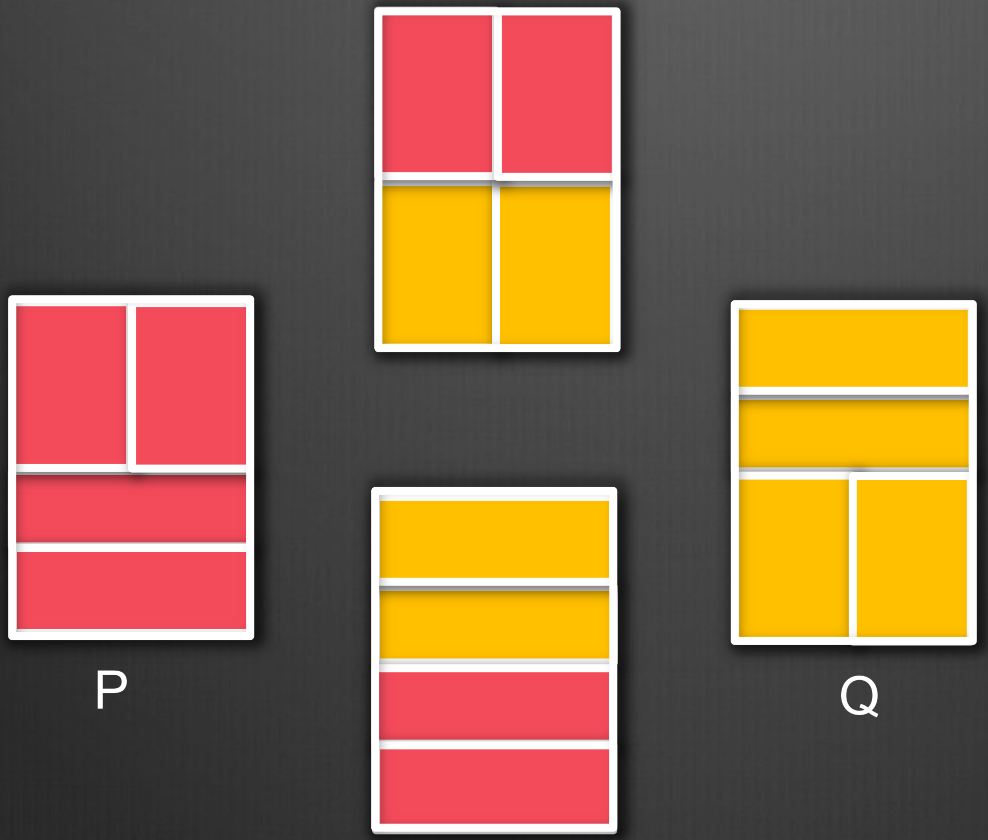
Tiling closure

Equivalence classes = observations

Tiling closure of a set of partitions = all relations that can be built by mixing and matching observations


P
Q


P
Q


P
Q

Conclusion

A Quantale of Information: a strict generalisation of the Lattice of Information

More in the paper, including:

- Capture the essence of ethical wall policies in a precise sense
- Nice compositional properties which make reasoning easier:

$$\frac{f_1 : \mathbb{P} \Rightarrow \mathbb{Q} \quad \mathbb{Q} \sqsupseteq \mathbb{Q}' \quad f_2 : \mathbb{Q}' \Rightarrow \mathbb{R}}{f_1; f_2 : \mathbb{P} \Rightarrow \mathbb{R}}$$