IFIP WG2.2, Singapore 13-16/9/16.

A demonic lattice of information

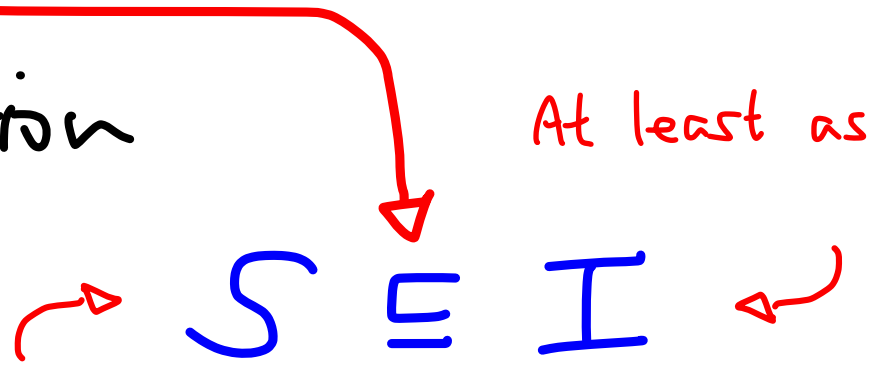
Carroll Morgan

University of NSW
+ Data61, CSIRO
+ Currently visiting ETHZ

Motivation and Context

Programming-language semantics for security based on principles of

> specification,
> refinement,
> implementation



The lattice of information

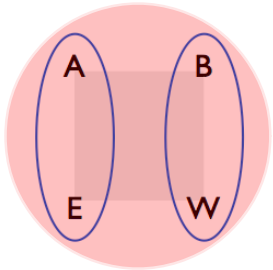
state space X of hidden values
observation function $f: X \to Y$
abstraction from observations Y
leaves the kernel of f
partitions form a lattice

its "essence"

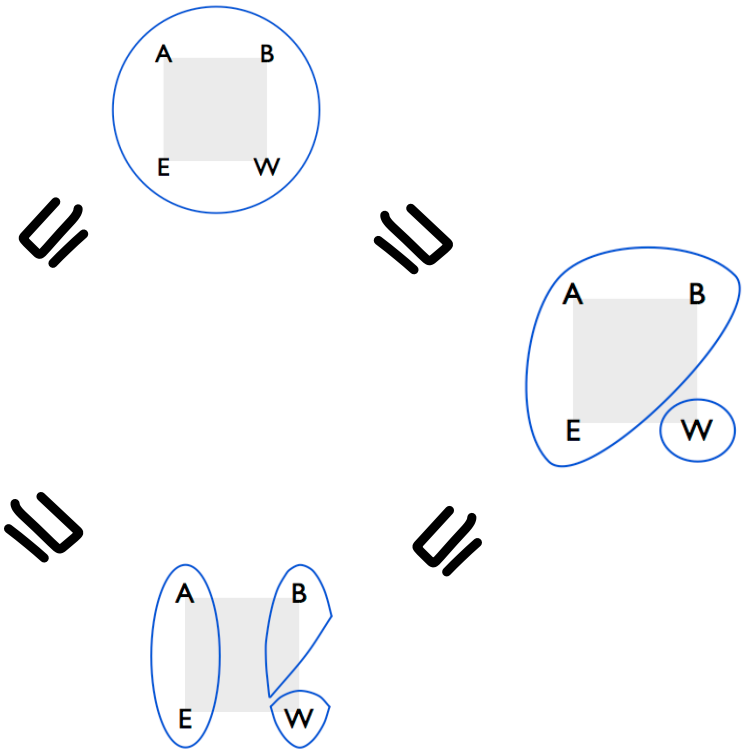
Landauer and Redmond, 1993.

Example

f_1 : A, E ↦ true
B, W ↦ false



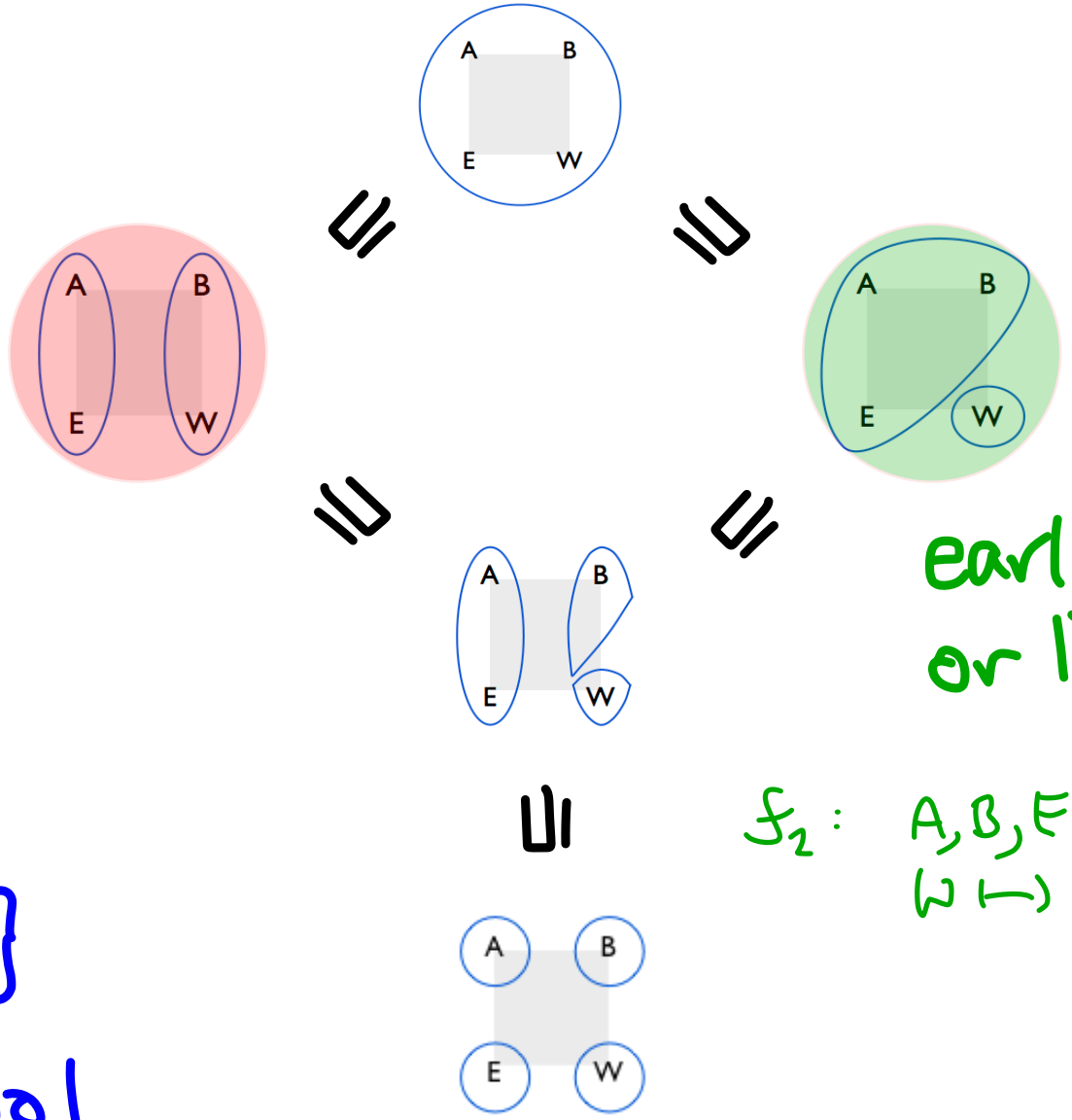
vowel or consonant ?



$X = \{A, B, E, W\}$

$f_1 : X \to Bool$

Example



early or late?

f_2: A, B, E ↦ true
W ↦ false

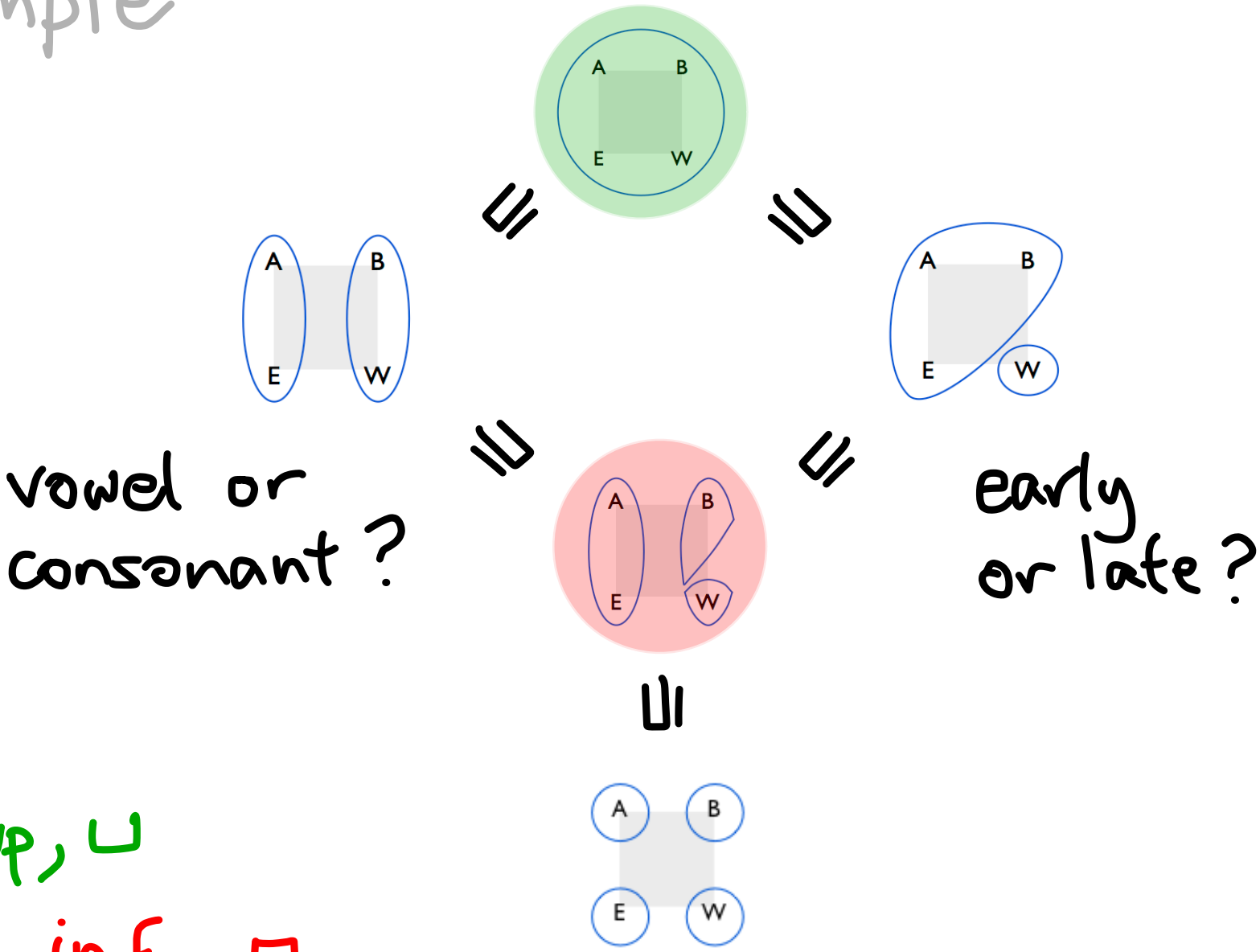
$X = \{A, B, E, W\}$

$f_2 : X \to \text{Bool}$

Example

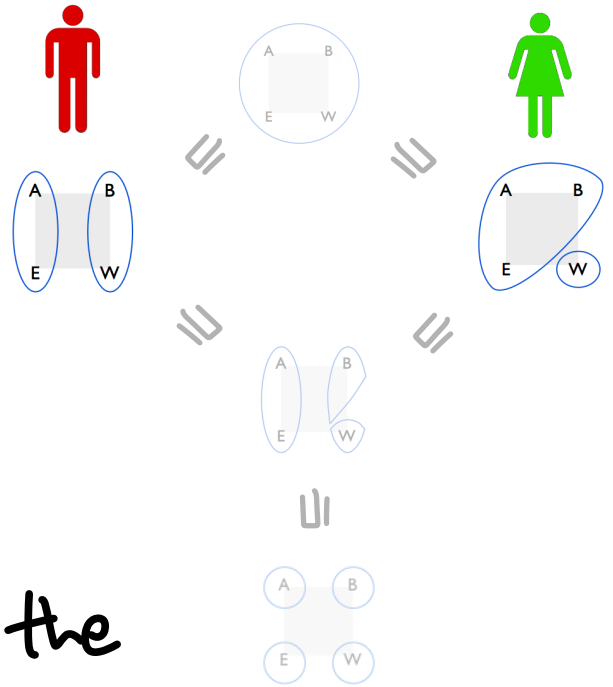
Still . . .

Landauer and Redmond, 1993.



But now...

Question



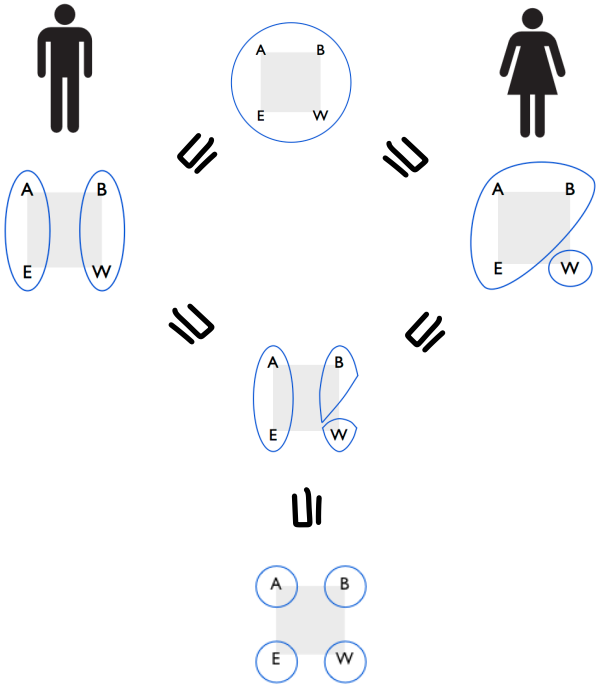
Two spies: Mr Vowel, Ms. Early.

1) Only one will return from the mission, but you don't know beforehand who it will be.

2) You receive a radio message from one of them, but you don't know who sent it.

How are these represented?

Question



Two spies: Mr Vowel, Ms. Early.

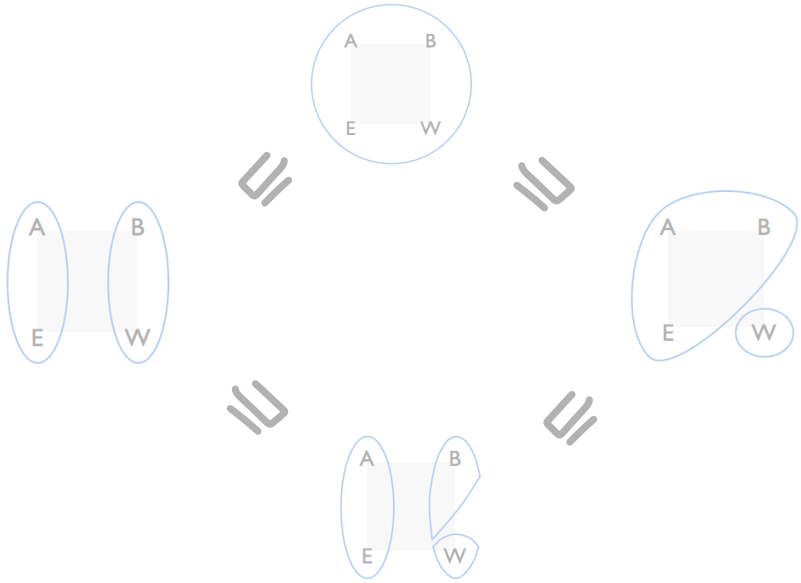
1) Only one will return from the mission, but you don't know beforehand which it will be.

2) You receive a radio message from one of them, but you don't know which one it was.

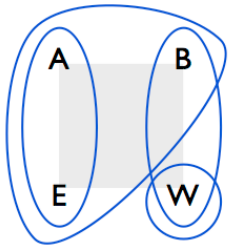
You receive T or F. In (1) you know who it was; in (2) you don't.

Answer

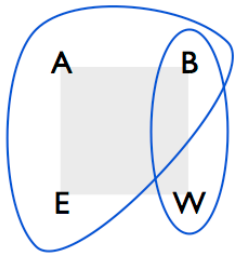
A demonic lattice of information



1) Only one will return from the mission, but you don't know beforehand which it will be.

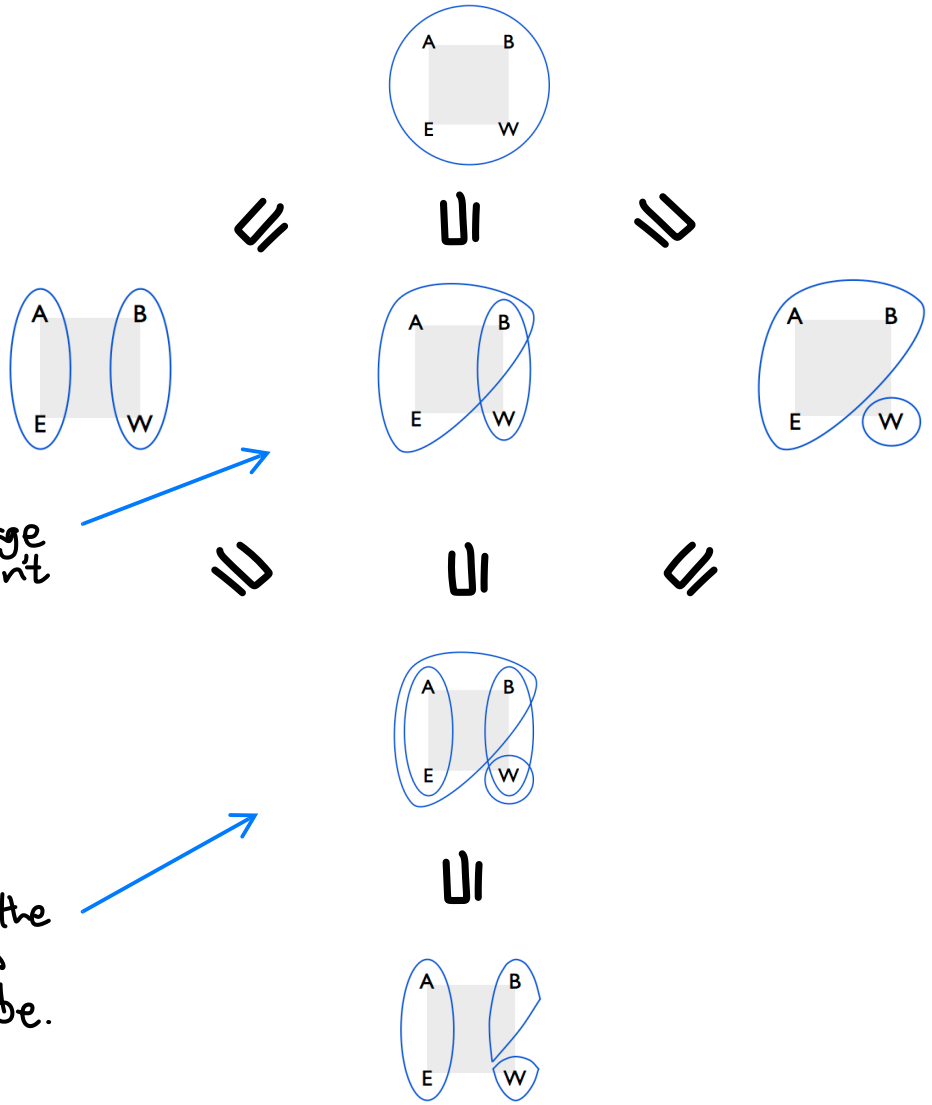


2) You receive a radio message from one of them, but you don't know which one it was.



Answer

A demonic lattice of information

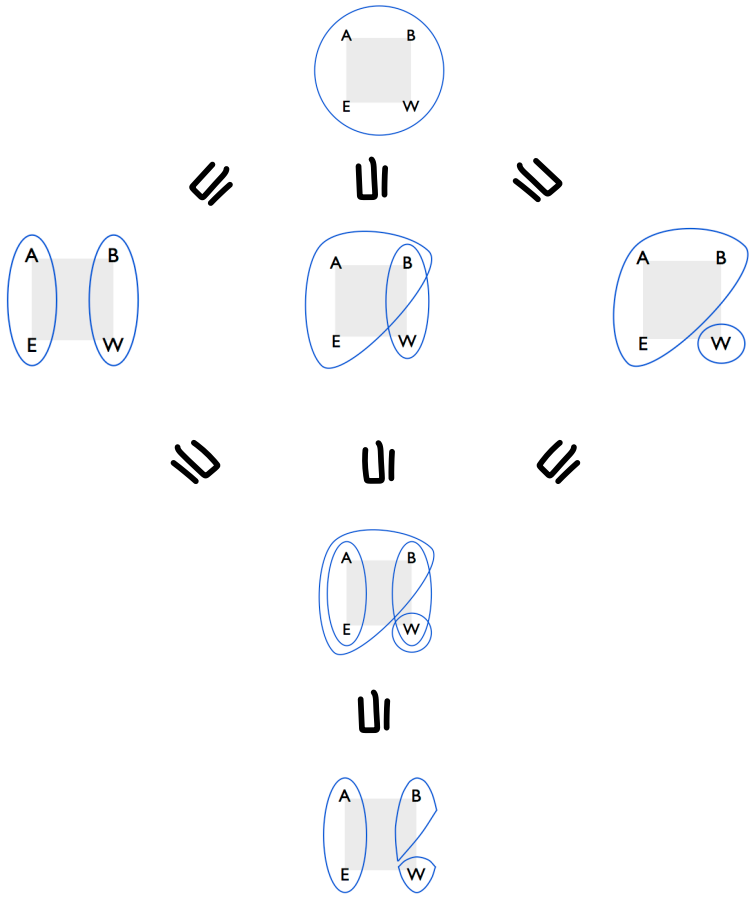


2) You receive a radio message from one of them, but you don't know which one it was.

1) Only one will return from the mission, but you don't know beforehand which it will be.

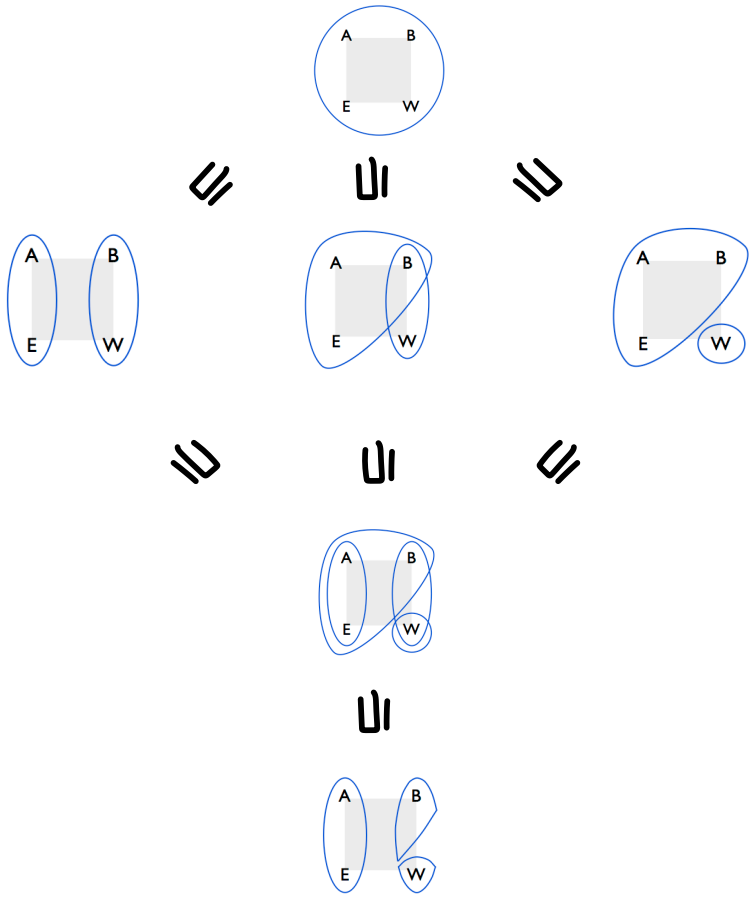
A demonic lattice of information

- What's the model?
- What's the order?
- What's compositionality?
- What are the tests?
- How do we justify our answers to the above?



A demonic lattice of information

- What's the model?

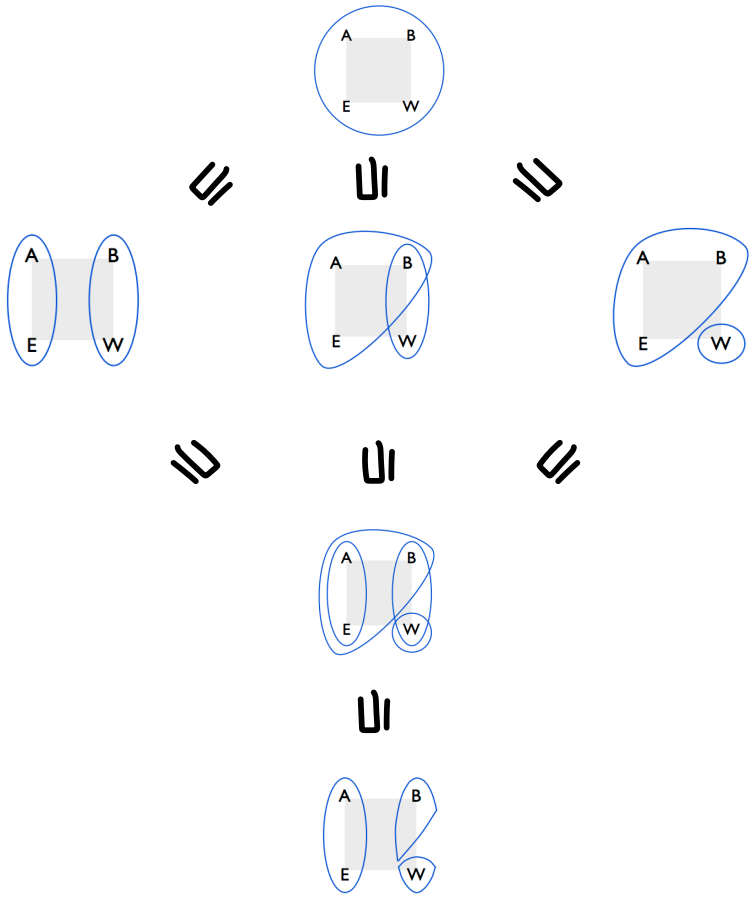


Union-closed covers of X.

The deterministic lattice is the special case of complement-closure as well.

A demonic lattice of information

- What's the order?

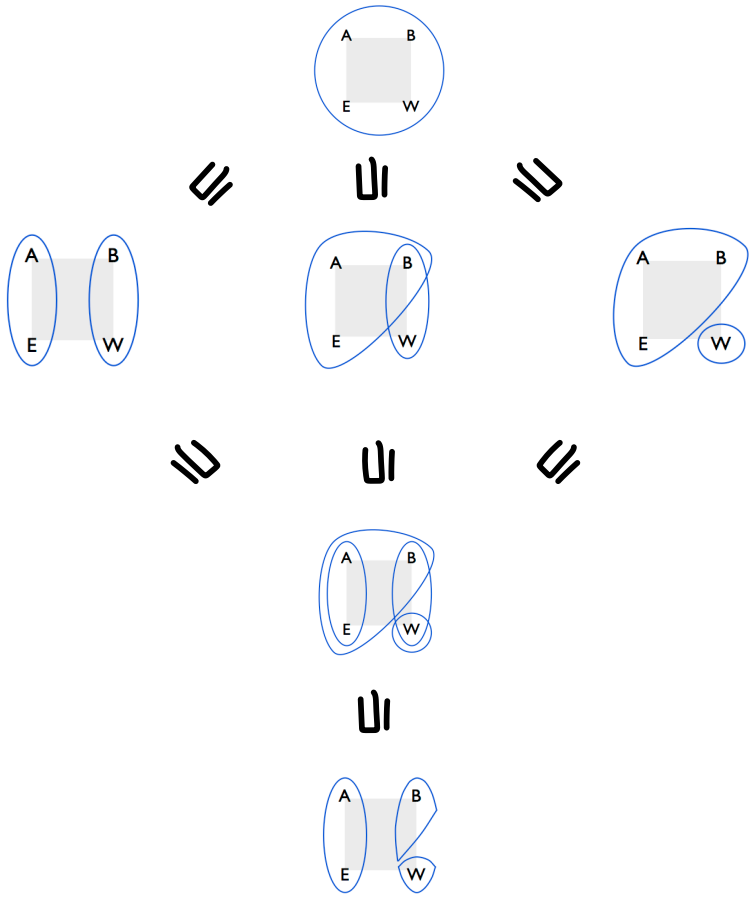


Reverse set-inclusion.

Without union-closure, it's Smyth-like: if $S \sqsubseteq I$ then every σ in I must be $\sigma_1 \cup \cdots \cup \sigma_N$ for some σ_n's in S.

A demonic lattice of information

- What's the order?



Sup is intersection.

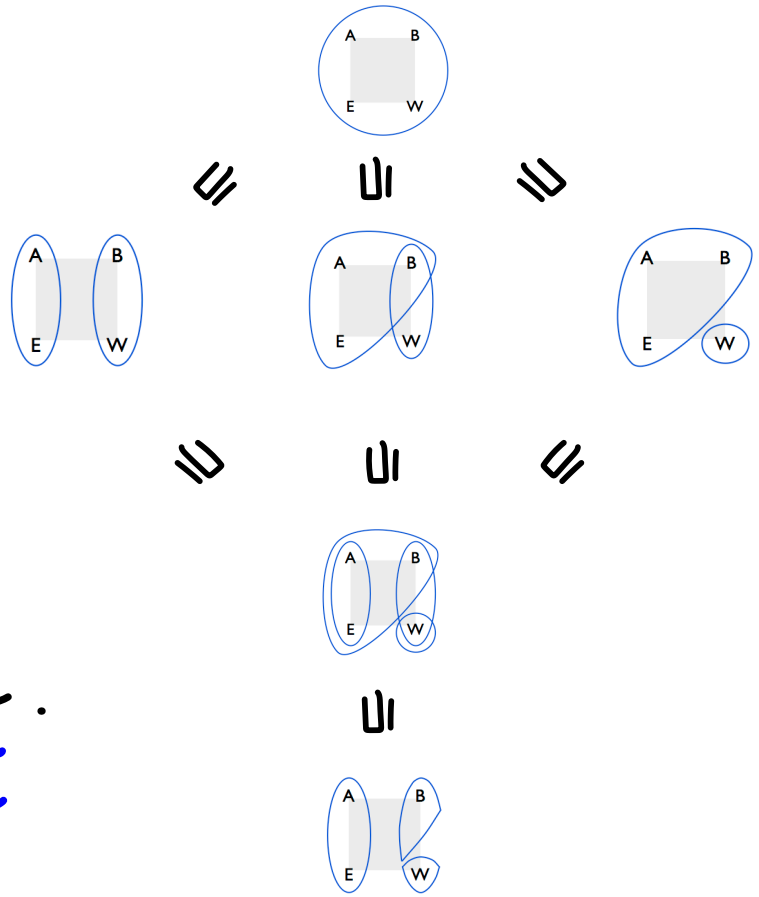
Inf is union followed by union closure.

A demonic lattice of information

- What's compositionality?

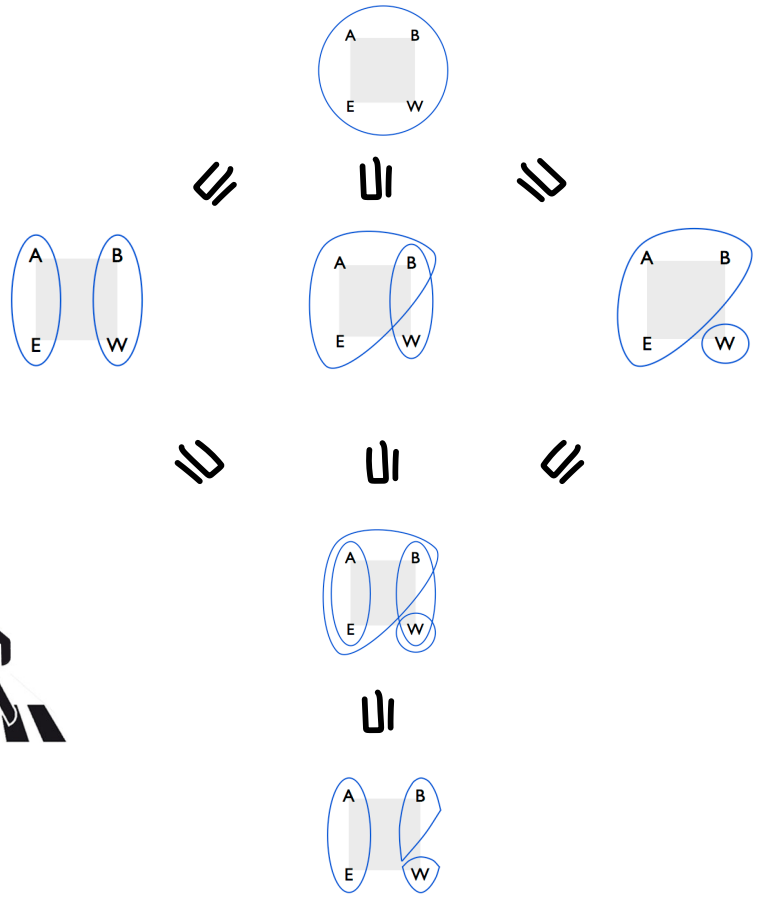
It depends on the composition.

We'll use $\|$, two spies attacking the same secret. Then we must have $S \sqsubseteq I$ implies $S \| C \sqsubseteq I \| C$ for any C.



A demonic lattice of information

- How do we justify our answers?



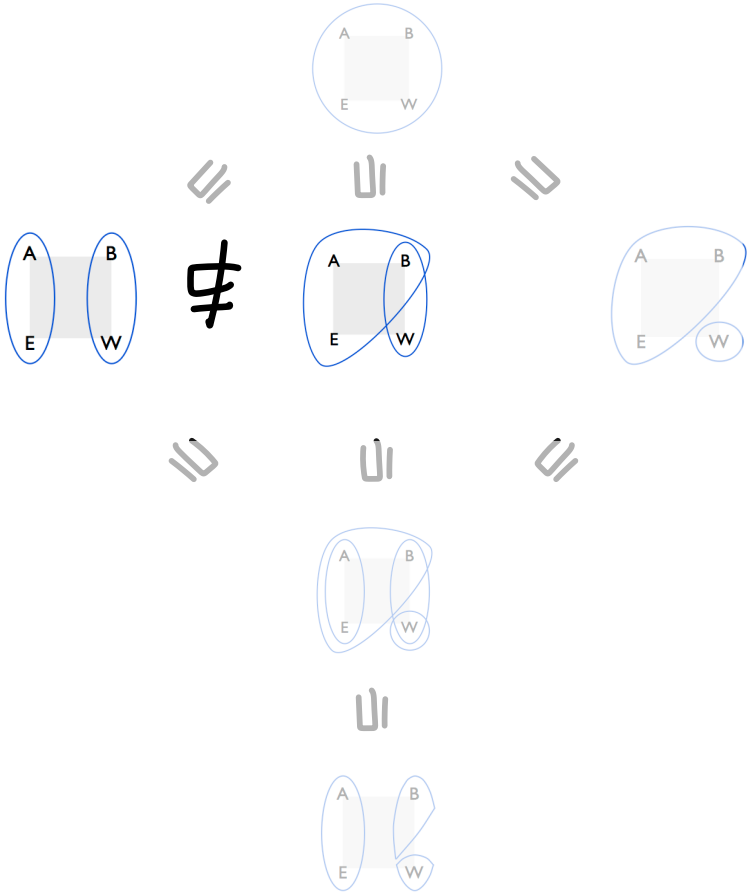
Compositional closure

Insist that $S \not\models K$ if K contains a singleton that S does not.

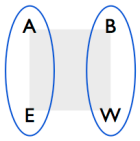
Take the largest sub $\subseteq$ that is compositional for $\amalg$.

A demonic lattice of information

- How do we justify our answers?



Run in parallel with

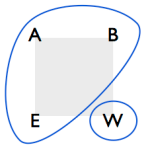


Insist that $S \not\subseteq K$ if K contains a singleton that S does not.

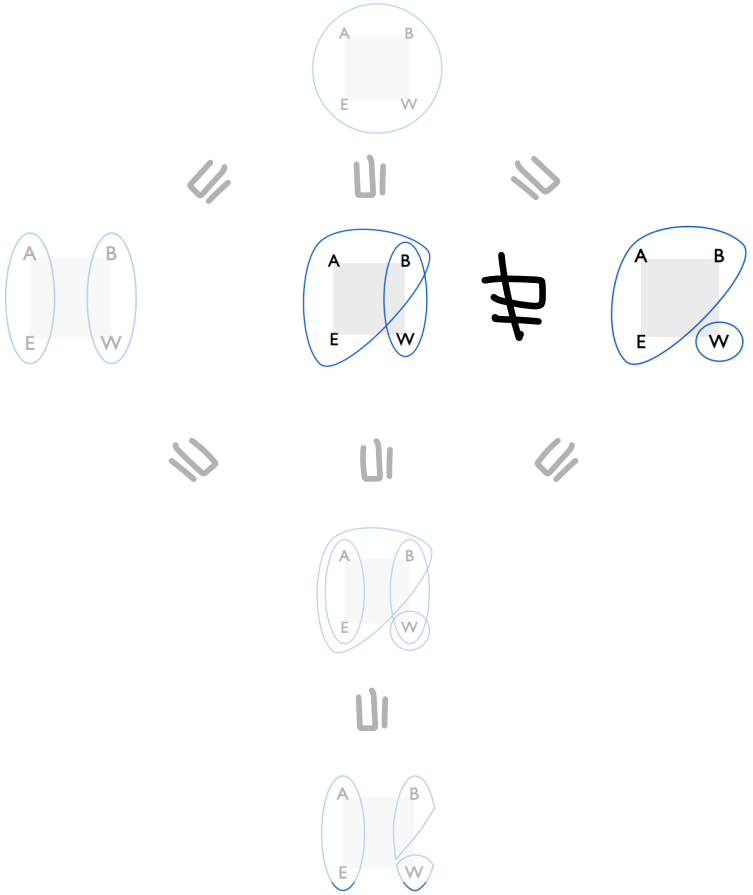
A demonic lattice of information

- How do we justify our answers?

Run in parallel with

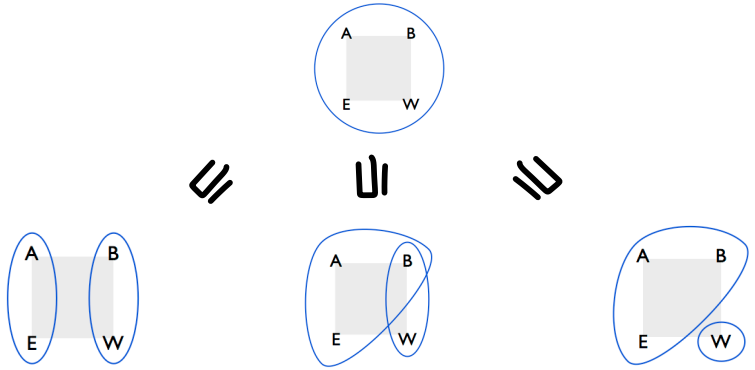


Insist that $S \not\sharp K$ if K contains a singleton that S does not.



A demonic lattice of information

- What are the tests?

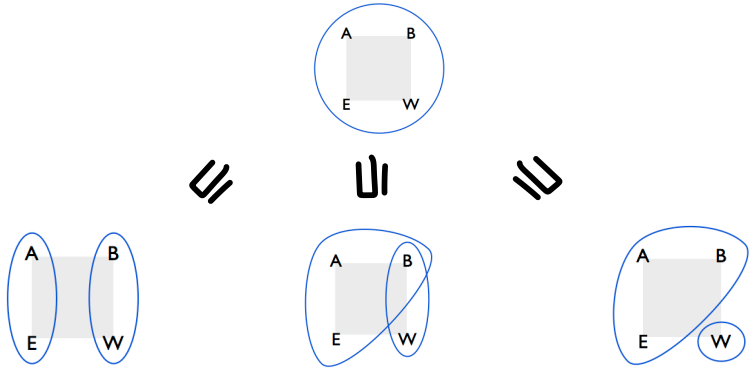


A specification S contains cells σ.
A cell σ either passes or fails a test Φ.
S passes Φ just when $(\forall \sigma : S \cdot \Phi(\sigma))$.

$S \not\equiv K$ if $\Phi(S)$ but $\neg\Phi(K)$ for some Φ.

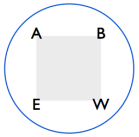
A demonic lattice of information

- What are the tests?

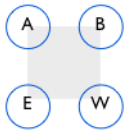


A test is a pair (A, C) of subsets.

Cell σ passes just when $\sigma \subseteq A \Rightarrow \sigma \subseteq C$.



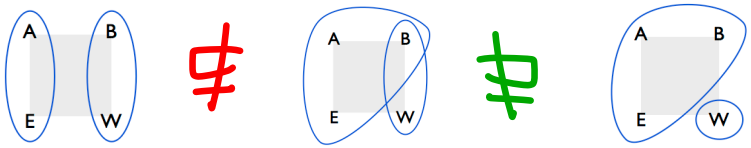
passes all non-trivial tests



fails all non-trivial tests

A demonic lattice of information

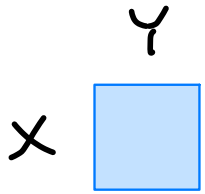
- What are the tests?



$(\subseteq\{A,B,E\}) \Rightarrow (\subseteq\{A,B\})$

$(\subseteq\{B,W\}) \Rightarrow (\subseteq\{W\})$

The surprise



All three models can be expressed as matrices:

- matrices with one 1 in each row
- matrices with at least one 1
- stochastic matrices.

When that is done, refinement is post matrix-multiplication by a "refinement matrix" of the same kind.

Applications

By adding state updates and control structures (eg. conditionals and loops) you find a monadic semantics for programs (ie. $S \to MS$) in which these fundamental representations of information flow, and its refinement, are embedded in all three cases.

equivalence classes

$$\mathcal{P}X \to \mathbb{E}X$$

deterministic

$$\mathbb{P}X \to \mathbb{P}^2X$$

demonic

hyper-distributions

$$\mathbb{D}X \to \mathbb{D}^2X$$

probabilistic

Deterministic	Landauer, Redmond 1993
Demonic	Morgan 2006
Probabilistic	Alvim, ChatzikoKolatis, McIver, Morgan, Palamidessi, Smith since 2010/2012