A nondeterministic lattice of information

Carroll Morgan
University of New South Wales, and NICTA
Sydney, AU
The essence of information flow

Landauer and Redmond, 1993:
A (deterministic) lattice of information

Alvim, Chatzikokolakis, Mclver, Morgan, Smith, Palamidessi, since 2012:
A (probabilistic) lattice of information
This talk: **filling the gap**

1. Landauer and Redmond, **1993:**
   
   A *(deterministic) lattice of information*

2. Alvim, Chatzikokolakis, McIver, Morgan, Smith, Palamidessi, since **2012:**
   
   A *(probabilistic) lattice of information*
   
   (not a lattice, actually: only a (C)PO)

3. **MPC 2015:**
   
   A *(demonic) lattice of information*
A (deterministic) lattice of information

Here, programs are deterministic functions from secrets to observables; and such a function induces an equivalence relation on the secrets (of producing the same observable).

Over a fixed space of secrets $X$, those ER’s (equivalently, partitions) have a well known lattice order (of partition refinement).

Landauer and Redmond explored the implications of this lattice for security.

... a long time ago

A (deterministic) lattice of information

State space $X$ is \{A,B,E,W\}.

This $f$ is “vowel or consonant”.

This $f$ is “early or late”.

Let the deterministic observation-function be $f$.

This is a constant function.

This $f$ is “vowel or consonant”.

This $f$ is “early or late”.

State space $X$ is \{A,B,E,W\}.
A (deterministic) **lattice** of information

This $f$ is “vowel or consonant”.

Let the deterministic observation-function be $f$.

This $f$ is “early or late”.

State space $X$ is $\{A,B,E,W\}$.

This $f$ is (MOD 4).
A (deterministic) lattice of information

refinement order of increasing security

less secure
A (deterministic) lattice of information
Merging: soundness and completeness

Suppose we have two partitions $S, I$ of state-space $\mathcal{X}$, and that $S, I$ are generated by observation functions $s: \mathcal{X} \to \mathcal{B}_S$ and $i: \mathcal{X} \to \mathcal{B}_I$ respectively. Then

soundness $S \sqsubseteq I$ if there is a “merging function” $m: \mathcal{B}_S \to \mathcal{B}_I$ such that $i = m \circ s$.

completeness $S \sqsubseteq I$ only if there is such an $m$. 

\[ \begin{array}{ccc}
\mathcal{X} & \xrightarrow{s} & \mathcal{B}_S \\
\downarrow & \mathrel{=} & \downarrow m \\
i & \xrightarrow{i} & \mathcal{B}_I
\end{array} \]
Observation as a (channel) matrix

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>💎</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>💎</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>💎</td>
<td>💎</td>
<td></td>
</tr>
<tr>
<td>W</td>
<td></td>
<td></td>
<td>💎</td>
<td>💎</td>
</tr>
</tbody>
</table>

State

One tick per row; possibly many ticks in a column.
Refinement as matrix multiplication

Refinement is characterised by matrix post-multiplication with a “merging matrix”. 
**A (probabilistic) lattice of information**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong></td>
<td>0.1</td>
<td>0.2</td>
<td>0.3</td>
<td>0.4</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td><strong>E</strong></td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
</tr>
<tr>
<td><strong>W</strong></td>
<td>0</td>
<td>0.5</td>
<td>0</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Each row’s probabilities sum to one: a stochastic matrix.
A (probabilistic) lattice of information

Assume incoming state is uniformly distributed.

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>E</th>
<th>W</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0.1/0.35</td>
<td>0.21</td>
<td>0.19</td>
<td>0.35</td>
</tr>
<tr>
<td>B</td>
<td>0</td>
<td>0</td>
<td>0.65</td>
<td>0</td>
</tr>
<tr>
<td>E</td>
<td>0.25/0.35</td>
<td>0.26</td>
<td>0.16</td>
<td>0.22</td>
</tr>
<tr>
<td>W</td>
<td>0</td>
<td>0.53</td>
<td>0</td>
<td>0.43</td>
</tr>
</tbody>
</table>

outer probabilities

\[ \sum = 1 \]
Refinement is characterised by matrix post-multiplication with a (now quantitative) “merging matrix” — this time all three matrices are stochastic.
A (demonic) lattice of information

Missing, in between, is an opportunity — having nondeterministic matrices with not a single 1 per row but rather at least one 1 per row, and consequentially sets of sets that are not necessarily partitions, that can possibly overlap.

This is the demonic lattice of information: it generalises the deterministic case; it is generalised by the probabilistic case. Instead of cells (of a partition, disjoint), we speak of “shadows” – possibly overlapping subsets of the state space each representing knowledge that has escaped.

I will discuss highlights of this model.
A (demonic) lattice of information

Missing, in between, is an opportunity — having nondeterministic matrices with not a single 1 per row but rather *at least one* 1 per row, and consequentially sets of sets that are *not necessarily partitions*, that can possibly overlap.

This is the *demonic lattice of information*: it generalises the deterministic case; it is generalised by the probabilistic case. Instead of cells (of a partition, disjoint), we speak of “shadows” – possibly overlapping subsets of the state space each representing knowledge that has escaped.

I will discuss highlights of this model.
A (demonic) lattice of information

The deterministic case generalises to the demonic case by allowing the partitions’ cells to overlap.

The nondeterministic case

The probabilistic PO specialises to the demonic case by abstracting the conditional posteriors (inners) to their supports.
What’s refinement here?
It’s not shadow-superset.

This is surprising.

Each shadow (subset of the state space) represents a possible state of knowledge of the adversary. (The multiplicity of shadows represents externally visible demonic choice.)

Suppose there are three coins: coin A has two heads; coin C has two tails; and B has one of each. The observation is the face that shows; the secret is “Which coin is it?”
Refinement is shadow union, not shadow-superset

This is surprising.

Each shadow (subset of the state space) represents a possible state of knowledge of the adversary. (The multiplicity of shadows represents externally visible demonic choice.)

Suppose there are three coins: coin A has two heads; coin C has two tails; and B has one of each. The observation is the face that shows; the secret is “Which coin is it?”
Observation as a (channel) matrix

<table>
<thead>
<tr>
<th>state</th>
<th>heads</th>
<th>tails</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>C</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

shadows, overlapping

unquantified nondeterminism
Is that system more secure than this?

<table>
<thead>
<tr>
<th>state</th>
<th>heads</th>
<th>tails</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>C</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

observation

shadows (disjoint)

nondeterminism removed
Is this system more secure?

<table>
<thead>
<tr>
<th>state</th>
<th>heads</th>
<th>tails</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>C</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Observation: shadows grow, and overlap.

Restore nondeterminism.
Refinement as matrix multiplication

Refinement is characterised by matrix post-multiplication with a "merging matrix", but this time all three matrices are demonic: all 0's or 1's; at least one 1 in each row.
A (demonic) lattice of information: the story so far

- The state-space is some non-empty $\mathcal{X}$.
- The \textit{semantic space} is then sets of subsets, “shadows” of $\mathcal{X}$. They do not have to cover all of $\mathcal{X}$; they do not have to be disjoint.
- The “healthiness condition” for these sets of shadows is \textit{union closure} (not superset closure).
- Refinement is then merely reverse inclusion wrt. these healthy sets of sets (as with other powerdomains).
Mr and Mrs Smyth and Mr and Mrs Jones are next-door neighbours. Each family has a locked mailbox by the street.

Adversary Albert knows that Mrs Smyth occasionally receives money in the post, and he would like to steal it.
Because the mailboxes are locked, however, he has to steal the whole box and then break it open in his garage, at home.

Albert watches the postman every day, waiting for his chance. The observable is the mailbox; the secret is the recipient.

The shadows for each delivered letter are \{S,s\} and \{J,j\}. When the shadow contains s, he will steal the Smyth-box. Except…
Mr Smyth is a **Mafia** boss

Except… If Albert happens to steal any of Mr Smyth’s mail,

he will be **killed**.

Thus Albert dares not risk stealing the Smyth’s mailbox, ever. And, as a result, **this system is secure against Albert**.

*The significance of reward/punishment for the adversary is something we have learned only recently from Quantitative Information Flow, i.e. from the probabilistic case: security wrt a particular adversary depends on his circumstances.*
Mr Smyth is a **Mafia** boss

Except… If Albert happens to steal any of Mr Smyth’s mail, he will be **killed**.

Thus Albert dares not risk stealing the Smyth’s mailbox, ever. And, as a result, this system is secure against Albert.

*The significance of reward/punishment for the adversary is something we have learned only recently from Quantitative Information Flow, i.e. from the probabilistic case: security wrt a particular adversary depends on his circumstances.*
Trajectory

MPC 2006 (SCP 2009) → 2008 → ICALP 2010 → LiCS 2012

(on notation)
SCP 2014
MPC 2012

MSCS 2014
CSF 2014
PoST 2014
LiCS 2015

“The Shadow”

Landauer
deterministic
demonic
demonic

QIF

MPC 2015
Trajectory

MPC 2006 (SCP 2009) ➔ 2008 ➔ ICALP 2010 ➔ LiCS 2012

MSCS 2014 ➔ CSF 2014 ➔ PoST 2014 ➔ LiCS 2015

Engelhardt Moses

“The Shadow”

Malacaria

Landauer

Malacaria

demonic

deterministic

MPC 2015

QIF

Meinicke

Mclver

FAC

FME

SCP

ICTAC

Rodin

QIF

Alvim

Chatzikokolakis

Espinoza

Smith

Palamidessi

influenced

collaborated

led to

Hoang Sloane Wen

Rabehaja
Mrs Smyth finds out about Mr Smyth

When Mrs Smyth discovers Mr Smyth’s Mafia connections, she divorces him and resumes her maiden name: she becomes Ms Jones.

For a while, her mail continues to be delivered to her old address: the mailbox now reads

Mr Smyth and Ms Jones.

Unfortunately, the postman sometimes gets confused, and puts Ms Jones’ mail in the wrong box.

The shadows are now \{S,s\} and \{s,J,j\}, representing an increase of ignorance. Yet the system has become insecure against Albert, because he is prepared to steal the Jones’s mailbox. Earlier, he was not.
Mrs Smyth finds out about Mr Smyth

When Mrs Smyth discovers Mr Smyth’s Mafia connections, she divorces him and resumes her maiden name: she becomes Ms Jones.

For a while, her mail continues to be delivered to her old address: the mailbox now reads Mr Smyth and Ms Jones.

Unfortunately, the postman sometimes gets confused, and puts Ms Jones’ mail in the wrong box.

The shadows are now \{S,s\} and \{s,J,j\}, representing an increase of ignorance. Yet the system has become insecure against Albert, because he is prepared to steal the Jones’s mailbox. Earlier, he was not.
Let program $Spec$ be $x:\in\{0,1\} \sqcap x:\in\{2,3\}$, where ($:\in\$) is “internal demonic choice”, not observable (like choosing a recipient) and ($\sqcap\$) is “external demonic choice”, observable (like choosing a mailbox).

Let program $Kludge$ be $x:\in\{0,1\} \sqcap x:\in\{1,2,3\}$, so that every shadow of $Kludge$ is a superset of some shadow of $Spec$.

Then $Kludge; \ print x\div 2$ might reveal that $x=1$; but $Spec; \ print x\div 2$ never can.
And in case you don’t believe in fairytales

Let program $Spec$ be $x \in \{0, 1\} \sqcap x \in \{2, 3\}$, where $(\in)$ is “internal demonic choice”, not observable (like flipping a coin or rolling a die) and $(\sqcap)$ is “external demonic choice”, observable (like choosing between the coin and the die in the first place).

Let program $Kludge$ be $x \in \{0, 1\} \sqcap x \in \{1, 2, 3\}$, so that every shadow of $Kludge$ is a superset of some shadow of $Spec$.

Then $Kludge;\ print\ x \div 2$ might reveal that $x=1$; but $Spec;\ print\ x \div 2$ never can.

That’s no fairytale: it’s real. It’s an example of the failure of compositionality, equivalently a failure of monotonicity wrt refinement.
What is refinement, then?

Refinement is done in two (optional) steps:

i. (possibly) Add shadows each of which is the union of shadows that are already there; and

ii. (possibly) Remove shadows.

With this partial order (of refinement) we have a lattice.

An easier way of looking at this (eventually) is to impose union-closure.
What is refinement, then?

Refinements are:
- say nothing
- say non-neg or nothing
- say non-pos or nothing
- say *nn* or *np* or nothing

But this one is not a refinement.
The demonic lattice: a very quick tour

i. Union-closed sets of shadows can be taken the model; but what are the tests?

ii. Given the tests, what’s soundness and completeness for testing in this case?

iii. Can the tests be expressed in terms of program variables?

iv. Can we achieve source-level reasoning for this kind of non-interference security?
Union-closed sets of shadows is the model; but what are the tests?

A test is a pair of sets $A, C$ — and a shadow $S$ passes such a test just if

$$S \text{ is a subset of } C \text{ whenever } S \subseteq A \implies S \subseteq C.$$

Any $A, C$ are allowed. For example if $A$ and $C$ don’t intersect, then it simply means that the pair $(A, C)$ is satisfied only by the empty $S$. 
“Synthesis” of the $A,C$-test

$$Spc \not\subseteq Kld$$

$$\equiv (\exists \text{ shadow } K:Kld \cdot K \notin Spc)$$

$$\equiv \text{“Spc union-closed”}$$

$$\equiv (\exists K:Kld \cdot (\exists k:K \cdot (\forall \text{ shadow } S:Spc \cdot k \in S \Rightarrow S \not\subseteq K)))$$

$$\equiv (\exists K:Kld; k \cdot k \in K \land (\forall \text{ shadow } S:Spc \cdot k \in S \Rightarrow S \not\subseteq K)))$$

$$\equiv \text{“define } \Phi_{A,C}(X) := X \subseteq A \Rightarrow X \subseteq C')$$

$$\equiv (\exists K:Kld; k \cdot \neg \Phi_{K,\overline{k}}(K) \land (\forall S:Spc \cdot \Phi_{K,\overline{k}}(S)))$$

$$\equiv (\exists K:Kld; \text{ test } \Phi \cdot \neg \Phi(K) \land (\forall S:Spc \cdot \Phi(S)))$$

“if” here requires a moment’s thought.
Given the tests, what’s soundness and completeness for testing in this case?

• If $Spec$ is refined by $Imp$, then every test passed by all shadows of $Spec$ must also be passed by all shadows of $Imp$.

• If $Kludge$ does not refine $Spec$, then there is a test that all shadows of $Spec$ pass, but some shadow of $Imp$ fails.

• Any collection of tests characterises a union-closed set of shadows.

• Any union-closed set of shadows is characterised by some collection of tests.
“Synthesis” of the $A,C$ -test

$Spc \not\subseteq Kld$

$\equiv (\exists \text{ shadow } K:Kld \cdot K \not\in Spc)$
$\equiv \text{ “Spc union-closed”}$
$\quad (\exists K:Kld \cdot \forall \text{ shadow } S:Spc \cdot k \in S \Rightarrow S \not\subseteq K))$

$\equiv (\exists K:Kld; k \cdot k \in K \land$
$\quad (\forall \text{ shadow } S:Spc \cdot k \in S \Rightarrow S \not\subseteq K))$

$\equiv \text{ “define } \Phi_{A,C}(X) := X \subseteq A \Rightarrow X \subseteq C’”$
$\quad (\exists K:Kld; k \cdot \neg \Phi_{K,k}(K) \land (\forall S:Spc \cdot \Phi_{K,k}(S)))$

$\equiv (\exists K:Kld; \text{ test } \Phi \cdot \neg \Phi(K) \land (\forall S:Spc \cdot \Phi(S)))$

“if” here requires a moment’s thought.
The demonic lattice: a very quick tour

*Can the tests be expressed in terms of program variables?*

When $A$ and $C$ are given as predicates over the program variables, say formulae $\Phi$ and $\Psi$ rather than set expressions, then “being a subset” is implication, universally quantified over those program variables.
The demonic lattice: a very quick tour

Can the tests be expressed in terms of program variables?

And that is a a very familiar paradigm for those used to assertional reasoning over program texts.

The shadow’s being a “subset” of some predicate $Phi$ can be thought of as a modal formula $KPhi$, that is that “$Phi$ is known to hold for all states in the shadow”.

Its dual is $PPhi$, that “It is not known that $A$ doesn’t hold for some state in the shadow.”
Idioms and examples

We use state variables $x, y, \ldots$ and a state-space $\mathcal{X} \times \mathcal{Y} \times \cdots$ as appropriate.

- $x$'s exact value is unknown: $(\forall x: \mathcal{X} \cdot K(x=x) \Rightarrow K \bot)$
- Nothing is known about $x$: $(\forall x: \mathcal{X} \cdot K(x \neq x) \Rightarrow K \bot)$
- Neither $x$'s nor $y$'s exact value is known:
  $$(\forall x: \mathcal{X}; y: \mathcal{Y} \cdot (K(x=x) \Rightarrow K \bot) \land (K(y=y) \Rightarrow K \bot))$$
- Learning $x$'s value does not reveal $y$'s value:
  $$(\forall x: \mathcal{X}; y: \mathcal{Y} \cdot K(x=x \Rightarrow y=y) \Rightarrow K(x \neq x))$$
- Learning $x$'s value does not reveal anything about $y$:
  $$(\forall x: \mathcal{X}; y: \mathcal{Y} \cdot K(x=x \Rightarrow y \neq y) \Rightarrow K(x \neq x))$$

We use $\top$ for true and $\bot$ for false.
Idioms and examples

We use state variables $x, y, \ldots$ and a state-space $\mathcal{X} \times \mathcal{Y} \times \cdots$ as appropriate.

- $x$’s exact value is unknown ($\forall x: \mathcal{X} \cdot K(x=x) \Rightarrow K \bot$)
- nothing is known about $x$ ($\forall x: \mathcal{X} \cdot K(x\neq x) \Rightarrow K \bot$)
- neither $x$’s nor $y$’s exact value is known ($\forall x: \mathcal{X}; y: \mathcal{Y} \cdot (K(x=x) \Rightarrow K \bot) \land (K(y=y) \Rightarrow K \bot)$)
- learning $x$’s value does not reveal $y$’s value ($\forall x: \mathcal{X}; y: \mathcal{Y} \cdot K(x=x \Rightarrow y=y) \Rightarrow K(x\neq x)$)
- learning $x$’s value does not reveal anything about $y$ ($\forall x: \mathcal{X}; y: \mathcal{Y} \cdot K(x=x \Rightarrow y\neq y) \Rightarrow K(x\neq x)$)
Idioms and examples

We use state variables \( x, y, \ldots \) and a state-space \( \mathcal{X} \times \mathcal{Y} \times \cdots \) as appropriate.

- \( x \)'s exact value is unknown  
  \( (\forall x: \mathcal{X} \cdot K(x=x) \Rightarrow K \bot) \)

- Nothing is known about \( x \)  
  \( (\forall x: \mathcal{X} \cdot K(x\not=x) \Rightarrow K \bot) \)

- Neither \( x \)'s nor \( y \)'s exact value is known  
  \( (\forall x: \mathcal{X}; y: \mathcal{Y} \cdot (K(x=x) \Rightarrow K \bot) \land (K(y=y) \Rightarrow K \bot)) \)

- Learning \( x \)'s value does not reveal \( y \)'s value  
  \( (\forall x: \mathcal{X}; y: \mathcal{Y} \cdot K(x=x \Rightarrow y=y) \Rightarrow K(x\not=x)) \)

- Learning \( x \)'s value does not reveal anything about \( y \)  
  \( (\forall x: \mathcal{X}; y: \mathcal{Y} \cdot K(x=x \Rightarrow y\not=y) \Rightarrow K(x\not=x)) \)
Idioms and examples

We use state variables $x, y, \ldots$ and a state-space $\mathcal{X} \times \mathcal{Y} \times \cdots$ as appropriate.

$x$’s exact value is unknown $\quad (\forall x : \mathcal{X} \cdot K(x=x) \Rightarrow K \bot)$
nothing is known about $x$ $\quad (\forall x : \mathcal{X} \cdot K(x \neq x) \Rightarrow K \bot)$
neither $x$’s nor $y$’s exact value is known $(\forall x : \mathcal{X}; y : \mathcal{Y} \cdot (K(x=x) \Rightarrow K \bot) \land (K(y=y) \Rightarrow K \bot))$
learning $x$’s value does not reveal $y$’s value $(\forall x : \mathcal{X}; y : \mathcal{Y} \cdot K(x=x \Rightarrow y=y) \Rightarrow K(x \neq x))$
learning $x$’s value does not reveal anything about $y$ $(\forall x : \mathcal{X}; y : \mathcal{Y} \cdot K(x=x \Rightarrow y \neq y) \Rightarrow K(x \neq x))$
Idioms and examples

We use state variables $x, y, \ldots$ and a state-space $\mathcal{X} \times \mathcal{Y} \times \cdots$ as appropriate.

$x$'s exact value is unknown $(\forall x: \mathcal{X} \cdot K(x=x) \Rightarrow K \bot)$
nothing is known about $x$ $(\forall x: \mathcal{X} \cdot K(x\neq x) \Rightarrow K \bot)$
neither $x$'s nor $y$'s exact value is known $(\forall x: \mathcal{X}; y: \mathcal{Y} \cdot (K(x=x) \Rightarrow K \bot) \land (K(y=y) \Rightarrow K \bot))$
learning $x$'s value does not reveal $y$'s value $(\forall x: \mathcal{X}; y: \mathcal{Y} \cdot K(x=x \Rightarrow y=y) \Rightarrow K(x\neq x))$
learning $x$'s value does not reveal anything about $y$ $(\forall x: \mathcal{X}; y: \mathcal{Y} \cdot K(x=x \Rightarrow y\neq y) \Rightarrow K(x\neq x))$

Do we really understand the English here?
Idioms and examples

if $x$ is not 0, then in fact it’s not 1 (either) $K(x \neq 0) \Rightarrow K(x \neq 1)$

—(ditto)— $K\{1, 2, 3\} \Rightarrow K\{2, 3\}$

if we know the letter was not for Mr. Smyth, then we know it was not for Mrs. Smyth

$K(\text{not for Mr. Smyth}) \Rightarrow K(\text{not for Mrs. Smyth})$

equivalently $P(\text{for Mrs. Smyth}) \Rightarrow P(\text{for Mr. Smyth})$

The Mr/Mrs Smyth assertion is satisfied by the Mrs. Smyth system but not by the Ms. Jones system: it shows therefore that the latter does not refine the former.
Hey, there’s no idiom for that…

Only properties that are preserved by refinement can be expressed in this form, that is as conjunctions of $K$-implications (equiv. of $P$-implications). And every property that is refinement preserving can be expressed that way. As with all formal methods, our hope here is that this rigour is limiting our vocabulary to statements that actually make sense for refinement. And any property not preserved by refinement does not make sense, at least not for serious program development.

Expressively complete

And every failed refinement can be caught by a single $K$-pair or $P$-pair.
The demonic lattice: a very quick tour

Can we achieve source-level reasoning for this kind of non-interference security?

Yes. Although it can be intricate, at least it’s mechanical.

- For `wp.assignment.Ph`i replace every $K(\text{body})$ in Phi with $K(wp.assignment.body)$
- For external demonic choice, take the conjunction.
- For `wp.(print exp).Phi` replace every $K(\text{body})$ in Phi with $K(exp=x \Rightarrow \text{body})$ and put $(\forall x \ldots)$ on the outside.

\[
P\Phi = \neg K(\neg \Phi) \text{ becomes } \neg K(\Psi \Rightarrow \neg \Phi) = P(\Psi \land \Phi)
\]
Refinements... and not

\[ \text{Prog}_1 \cap \text{Prog}_2 \subseteq \text{Prog}_1 \]

because

\[ \text{wp.}(\text{Prog}_1 \cap \text{Prog}_2).\Phi \]

\[ \Rightarrow \text{wp.}	ext{Prog}_1.\Phi \]

\[ = \text{wp.}	ext{Prog}_1.\Phi \land \text{wp.}	ext{Prog}_2.\Phi \]

so that e.g. we have \( x := 1 \cap x := 2 \subseteq x := 1 \).

But we never have \( x \in S_1 \subseteq x \in S_2 \) unless \( S_1 = S_2 \).

Why not?

The Refinement Paradox
External demonic choice represents (as usual) implementation freedom, deliberate looseness in a specification, run-time unpredictability…

and it can be “refined away” to a more constrained implementation, a tighter specification, or more predictable behaviour at run-time.

Refinement can make $EDC$ smaller, but never larger.
External- vs. **internal** demonic choice

**Internal** demonic choice represents deliberate obfuscation. It can’t be reduced, because that would reduce security as well (e.g. fewer possible passwords).

But in general it can’t be increased either, because that might consequentially cause an increase in external nondeterminism. For example, sticking a “more secure” 10-character password into an 8-byte field actually decreases security: buffer overrun.

Refinement in general cannot change **IDC** in either direction: not smaller, not larger.
Internal demonic choice represents deliberate obfuscation. It can’t be reduced, because that would reduce security as well (e.g. fewer possible passwords).

But in general it can’t be increased either, because that might consequentially cause an increase in external nondeterminism. For example, sticking a “more secure” 10-character password into an 8-byte field actually decreases security: buffer overrun.

Refinement in general cannot change IDC in either direction: not smaller, not larger.
How changing \( IDC \) is prevented

Suppose \( \text{wp.}(x:\in S). (K\Psi \Rightarrow K\Phi) \) holds. That is by definition

\[
K(\text{wp.}(x:\in S).\Psi) \Rightarrow K(\text{wp.}(x:\in S).\Phi).
\]

If \( S \) is made larger, the antecedent and the consequent both become stronger; if \( S \) is made smaller, the antecedent and the consequent both become weaker. Neither of those is implication in general.
How changing IDC is detected

Programs $x \in S_1$ and $x \in S_2$ have as results the single shadows $S_1$ and $S_2$ resp. What single test distinguishes them when $S_1 \neq S_2$?

If $S_2 \not\subset S_1$ then $S_1$ passes $K \top \Rightarrow KS_1$ but $S_2$ does not.
If $S_2 \subset S_1$ then $S_1$ passes $KS_2 \Rightarrow K \bot$ but $S_2$ does not.

Either way we have $x \in S_1 \nsubseteq x \in S_2$. 
Examples of source-level reasoning

\[
\begin{align*}
\text{wp.}(x:=x+1).\text{“don’t know } x \text{ is even”} \\
= \quad \text{wp.}(x:=x+1).\ (K(x \text{ is even}) \Rightarrow K\bot) \\
= \quad K(\text{wp.}(x:=x+1).(x \text{ is even})) \Rightarrow K(\text{wp.}(x:=x+1).\bot) \\
= \quad K(x \text{ is odd}) \Rightarrow K\bot \\
= \quad \text{“don’t know } x \text{ is odd”}.
\end{align*}
\]

Deterministic.
Examples of source-level reasoning

\[
\text{wp.}(x \leftarrow x+1 \sqcap \text{skip}).\text{“don’t know } x \text{ is even”}
\]

\[
= \text{wp.}(x \leftarrow x+1).\left( K(x \text{ is even}) \Rightarrow K \bot \right)
\]
\[
\quad \land \text{wp.skip.}(K(x \text{ is even}) \Rightarrow K \bot)
\]

\[
= K(\text{wp.(}x \leftarrow x+1).\left(x \text{ is even}) \Rightarrow K(\text{wp.(}x \leftarrow x+1).\bot)
\]
\[
\quad \land K(\text{wp.skip.}(x \text{ is even))) \Rightarrow K(\text{wp.skip.}\bot)
\]

\[
= (K(x \text{ is odd}) \Rightarrow K \bot) \land (K(x \text{ is even}) \Rightarrow K \bot)
\]

\[
= K(x \text{ is odd}) \lor K(x \text{ is even}) \Rightarrow K \bot
\]

\[
= (\exists z: \{0, 1\} \cdot K(x \mod 2 = z)) \Rightarrow K \bot
\]

\[
= \text{“don’t know } x \text{‘s parity”}.
\]

External nondeterminism is visible to the adversary.
Examples of source-level reasoning

Between statements this is $EDC$; within an expression it is $IDC$.

\[
\begin{align*}
wp.(x := (x+1) \sqcap x). \text{“don’t know } x \text{ is even”} \\
= \quad \quad \quad \quad \quad wp.(x := (x+1) \sqcap x). (K(x \text{ is even}) \Rightarrow K \bot) \\
= \quad \quad \quad \quad \quad K(wp.(x := (x+1) \sqcap x). (x \text{ is even})) \\
\Rightarrow \quad \quad \quad \quad \quad K(wp.(x := (x+1) \sqcap x). \bot) \\
= \quad \quad \quad \quad \quad K \bot \Rightarrow K \bot \\
= \quad \quad \quad \quad \quad \top.
\end{align*}
\]

Internal nondeterminism is hidden from the adversary.
Examples of source-level reasoning

\[ \text{wp.} (\text{print } x). \text{“don’t know } x=0” \quad \text{“} x \text{ might not be 0”} \]

\[ = \text{wp.} (\text{print } x). (K(x=0) \Rightarrow K \bot) \]

\[ = (\forall x \cdot K(x=x \Rightarrow x=0) \Rightarrow K(x=x \Rightarrow \bot)) \]

\[ = (\forall x \cdot K(x=x \Rightarrow x=0) \Rightarrow K(x \neq x)) \]

\[ = K(x \neq 0) \land (\forall x \cdot K(x=x \Rightarrow x=0) \Rightarrow K(x \neq x)) \]

\[ = K(x \neq 0) \land (\forall x \cdot K(x \neq x) \Rightarrow K(x \neq x)) \]

\[ = K(x \neq 0). \text{“} x \text{ can’t be 0”} \]

To ensure that an attacker will think \( x \text{ might not be 0} \) afterwards, you must ensure that \( x \) is \textit{definitely not 0} before.
Examples of source-level reasoning

\[ \text{wp.(print } x) \cdot \text{“don’t know } x \text{'s exact value”} \]
\[ = \text{wp.(print } x) \cdot (\forall x \cdot K(x=x) \Rightarrow K\bot) \]
\[ = (\forall x' \cdot (\forall x \cdot K(x=x' \Rightarrow x=x) \Rightarrow K(x=x' \Rightarrow \bot))) \]
\[ = (\forall x, x' \cdot K(x=x' \Rightarrow x=x) \Rightarrow K(x\neq x')) \]
\[ \Rightarrow (\forall x \cdot K(x=x \Rightarrow x=x) \Rightarrow K(x\neq x)) \]
\[ = (\forall x \cdot K(x\neq x)) \]
\[ = K(\forall x \cdot x\neq x) \quad \text{“} x \text{’ can’t be any value } x \text{ before.”} \]
\[ = K\bot . \]

It would indeed be a miracle if printing \( x \)'s value did not reveal \( x \)'s exact value.
Examples of source-level reasoning

Either $x$ or $y$ is printed, but we do not know which one it was. When can we figure out $y$’s value even so?

$$
\text{wp.}(\text{print } x \sqcap y). \text{“do not know } y\text{’s exact value”}
= \text{wp.}(\text{print } x \sqcap y). (\forall y \cdot K(y=y) \Rightarrow K \bot)
= (\forall y, z \cdot K((x=z \lor y=z) \Rightarrow y=y) \Rightarrow K(x \neq z \land y \neq z)),
$$

which is mysteriously complex. Does it have to be?

The nondeterminism above is internal, within the print statement: it is not observable.
Examples of source-level reasoning

\[
\begin{align*}
\text{wp.}(\text{print } x \sqcap y) & \text{.“do not know } y\text{’s exact value”} \\
= & \text{ wp.}(\text{print } x \sqcap y) \cdot (\forall y \cdot K(y=y) \Rightarrow K \bot) \\
= & (\forall y, z \cdot K((x=z \lor y=z) \Rightarrow y=y) \Rightarrow K(x \neq z \land y \neq z)) \\
\end{align*}
\]

Either \( x \) or \( y \) is printed, but we do not know which one it was. When can we figure out \( y \)’s value even so?

It should at least imply “we don’t know \( y \)’s value beforehand.” It does that.

It should imply “there is no value that \( y \) can take but \( x \) cannot.” It does that, too.

It even implies “there is no value that \( x \) can take but not \( y \) and which \( x \)-value determines \( y \) uniquely.
Examples of source-level reasoning

\[
\text{wp.}(\text{print } x \mathcal{\sqcap} y). \text{“do not know } y\text{’s exact value”}
= \text{wp.}(\text{print } x \mathcal{\sqcap} y). (\forall y \cdot K(y=y) \Rightarrow K \bot)
= (\forall y, z \cdot K((x=z \lor y=z) \Rightarrow y=y) \Rightarrow K(x \neq z \land y \neq z))
\]

It should at least imply “we don’t know y’s value beforehand.” It does that.

It should imply “there is no value that y can take but x cannot.” It does that, too.

It even implies “there is no value that x can take but not y and which x-value determines y uniquely.
Examples of source-level reasoning

\[
\text{wp.}(\text{print } x \sqcap y). \text{“do not know } y\text{’s exact value”} \\
= \text{wp.}(\text{print } x \sqcap y). (\forall y \cdot K(y = y) \Rightarrow K \bot) \\
= (\forall y, z \cdot K((x = z \lor y = z) \Rightarrow y = y) \Rightarrow K(x \neq z \land y \neq z))
\]

It should at least imply “we don’t know y’s value beforehand.” It does that.

It should imply “there is no value that y can take but x cannot.” It does that, too.

It even implies “there is no value that x can take but not y and which x-value determines y uniquely.
Examples of source-level reasoning

\[
\begin{align*}
\text{wp.}(\text{print } x \sqcap y). \text{“do not know y’s exact value”} &= \text{wp.}(\text{print } x \sqcap y). (\forall y \cdot K(y = y) \Rightarrow K \perp) \\
&= (\forall y, z \cdot K((x = z \vee y = z) \Rightarrow y = y) \Rightarrow K(x \neq z \land y \neq z))
\end{align*}
\]

It should at least imply “we don’t know y’s value beforehand.” It does that.

It should imply “there is no value that y can take but x cannot.” It does that, too.

It even implies “there is no value that x can take but not y and which x-value determines y uniquely.

But all that is still not enough.
Examples of source-level reasoning

\[
\text{wp.}(\text{print } x \sqcap y). \text{“do not know } y \text{'s exact value”}
\]
\[
= \text{wp.}(\text{print } x \sqcap y). (\forall y \cdot K(y=y) \Rightarrow K \bot)
\]
\[
= (\forall y, z \cdot K((x=z \lor y=z) \Rightarrow y=y) \Rightarrow K(x \neq z \land y \neq z))
\]

It should at least imply “we don’t know y’s value beforehand.” It does that.

It should imply “there is no value that y can take but x cannot.” It does that, too.

It even implies “there is no value that x can take but not y and which x-value determines y uniquely.

What if we know nothing about x,y except that they are equal?
Examples of source-level reasoning

\[
\text{wp.}(\text{print } x \sqcap y). \text{“do not know } y\text{’s exact value”}
\]
\[
= \text{wp.}(\text{print } x \sqcap y). (\forall y \cdot K(y=y) \Rightarrow K \bot)
\]
\[
= (\forall y, z \cdot K((x=z \lor y=z) \Rightarrow y=y) \Rightarrow K(x \neq z \land y \neq z))
\]
\[
= (\forall z \cdot (\exists y \cdot K((x=z \lor y=z) \Rightarrow y=y)) \Rightarrow K(x \neq z \land y \neq z))
\]
\[
= (\forall z \cdot P(x=z \lor y=z) \Rightarrow (\forall y \cdot K((x=z \lor y=z) \Rightarrow y=y)))
\]
\[
= (\forall z \cdot P(z \in \{x, y\}) \Rightarrow (\forall y \cdot K(z \in \{x, y\} \Rightarrow y=y)))
\]

i.e. “For every value (z) that x or y might take, there is no single value (y) determined for y.”

This is not rocket science — it’s just fiddling with sets. But it is very tricky!
Security in general is very tricky.
Conclusions

- **Union-closed sets** of shadows is our model for demonic non-interference security.
- It is a **lattice**: it generalises L&R’s lattice; it is generalised by hyper-distributions.
- Any non-refinement can be demonstrated with a single **primitive test** “If we know A then we (also) know C.”
- Conjunctions of primitive tests capture **all and only** union-closed sets of shadows.
- There is a **wp-calculus** for conjunctions of primitive tests.
- The wp-generated preconditions can be complex! Is that intrinsic to security, viz. inescapable?
Conclusions

• **Union-closed sets** of shadows is our model for demonic non-interference security.

• It is a **lattice**: it generalises L&R’s lattice; it is generalised by hyper-distributions.

• Any non-refinement can be demonstrated with a single **primitive test** “If we know A then we (also) know C.”

• Conjunctions of primitive tests capture **all and only** union-closed sets of shadows.

• There is a **wp-calculus** for conjunctions of primitive tests.

• The wp-generated preconditions can be complex! Is that intrinsic to security, viz. inescapable?
Conclusions

- **Union-closed sets** of shadows is our model for demonic non-interference security.
- It is a **lattice**: it generalises L&R’s lattice; it is generalised by hyper-distributions.
- Any non-refinement can be demonstrated with a single **primitive test** “If we know A then we (also) know C.”
- Conjunctions of primitive tests capture all and only union-closed sets of shadows.
- There is a **wp-calculus** for conjunctions of primitive tests.
- The wp-generated preconditions can be complex! Is that intrinsic to security, viz. inescapable?
Conclusions

- **Union-closed sets** of shadows is our model for demonic non-interference security.
- It is a **lattice**: it generalises L&R’s lattice; it is generalised by hyper-distributions.
- Any non-refinement can be demonstrated with a single **primitive test** “If we know A then we (also) know C.”
- Conjunctions of primitive tests capture **all and only** union-closed sets of shadows.
- There is a **wp-calculus** for conjunctions of primitive tests.
- The wp-generated preconditions can be complex! Is that intrinsic to security, viz. inescapable?
Conclusions

- **Union-closed sets** of shadows is our model for demonic non-interference security.

- It is a **lattice**: it generalises L&R’s lattice; it is generalised by hyper-distributions.

- Any non-refinement can be demonstrated with a single **primitive test** “If we know A then we (also) know C.”

- Conjunctions of primitive tests capture **all and only** union-closed sets of shadows.

- There is a **wp-calculus** for conjunctions of primitive tests.

- The wp-generated preconditions can be complex! Is that intrinsic to security, viz. inescapable? **Hmm...**
On principles...

**Deterministic** Landauer and Redmond’s (1993) original work provided the motivation. Their context was simple enough that principles were not explicitly necessary.

**Probabilistic** Hyper-distributions (2010–5) are sufficiently complex that principles are indispensable.

**Demonic** Shadows (2006) were complex enough to benefit from explicit principles, but still simple enough that ad-hoc progress could be made without.

Using principles from 2010–5 and motivation from 1993, we have put Shadows at their place in the hierarchy.