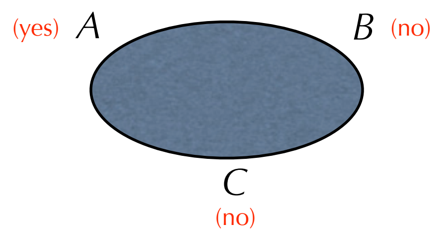
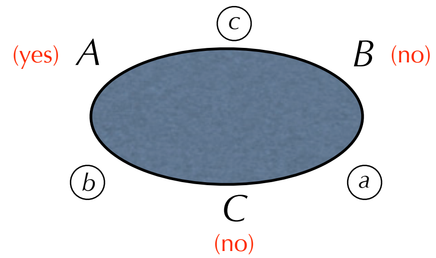
It's coffee-time in the Cryptographers' Café...

...and *A*,*B* and *C* have just finished having lunch. As usual, they amuse themselves by carrying out their favourite protocol: it determines whether one of them has already paid, but *without* revealing (if so) which who it was.



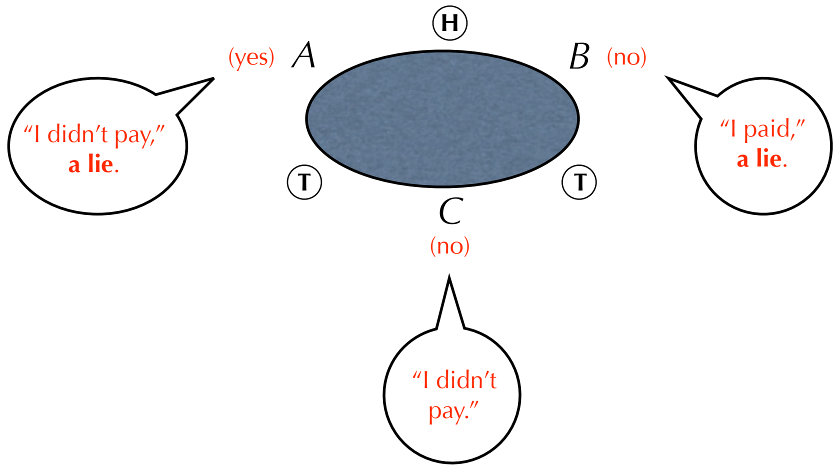
It's coffee-time in the Cryptographers' Café...

...and *A*,*B* and *C* have just finished having lunch. As usual, they amuse themselves by carrying out their favourite protocol: it determines whether one of them has already paid, but *without* revealing (if so) which it was.



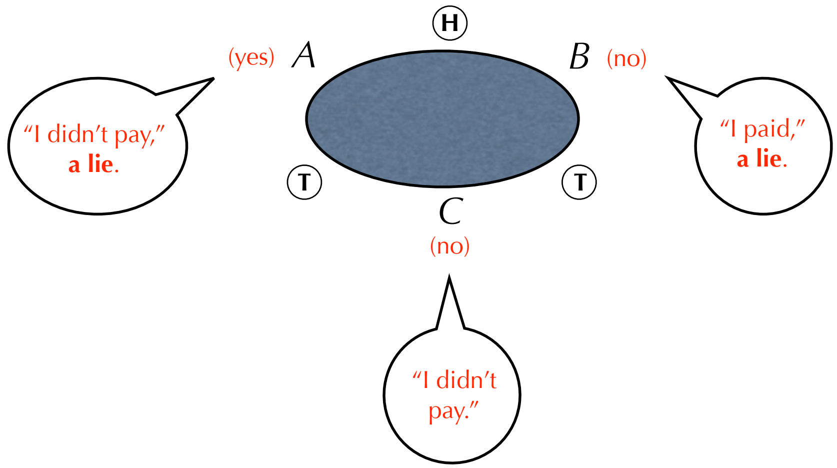
Between each pair is a coin out-of-sight of the third; the coin is flipped; and each cryptographer says whether she paid, *lying* however if the coins she sees are different.

It’s coffee-time in the Cryptographers’ Café...



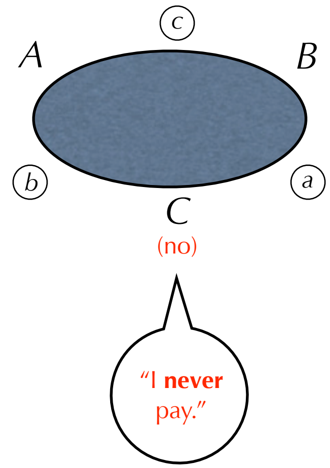
Between each pair is a coin out-of-sight of the third; the coin is flipped; and each cryptographer says whether she paid, *lying* however if the coins she sees are different.

It's coffee-time in the Cryptographers' Café...



Because an *odd number* claim to have paid, one of them actually did. But no-one (else) knows who, because none can see *both* coins that influenced the others' answers.

It's coffee-time in the Cryptographers' Café...



In that sense the *DCP* preserves the anonymity of its participants: it's a security-based correctness criterion.
But what if *C* says "I didn't pay" every single time?

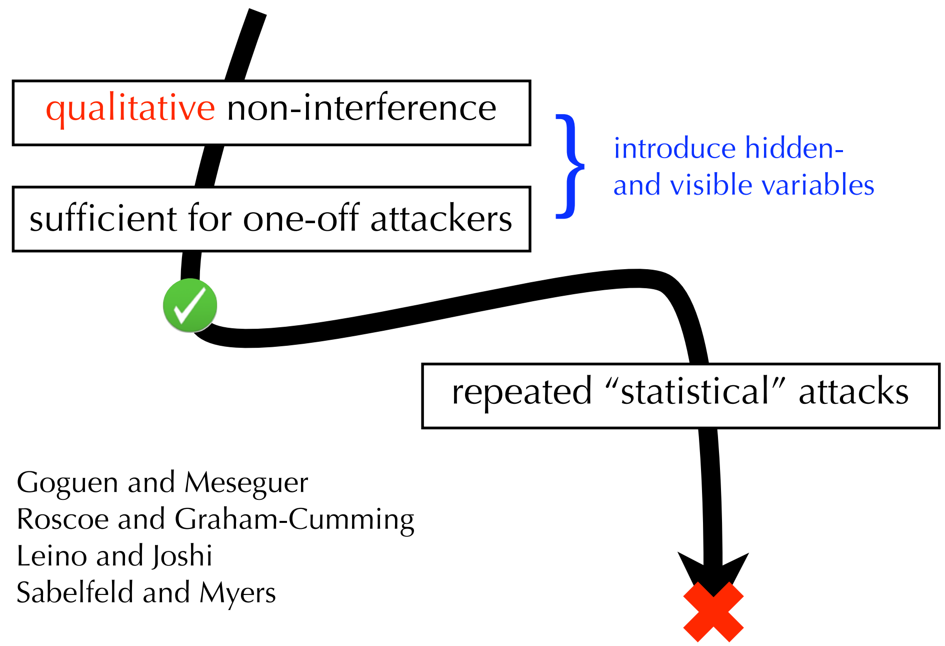
Summary: qualitative vs quantitative security

- Chaum's original article, including the correctness proof, specifies fair coins. We did not; but we proved correctness anyway...?
- Goguen and Meseguer's original article on non-interference does not mention probability either.
- Many proofs of security exist for the *DCP*, showcasing various computational security frameworks; many of those also do not mention probability.
- Yet under repeated trials (in the café, rather than for just a one-off lunch date), the protocol is not secure unless the coins are fair.

Summary: qualitative vs quantitative security

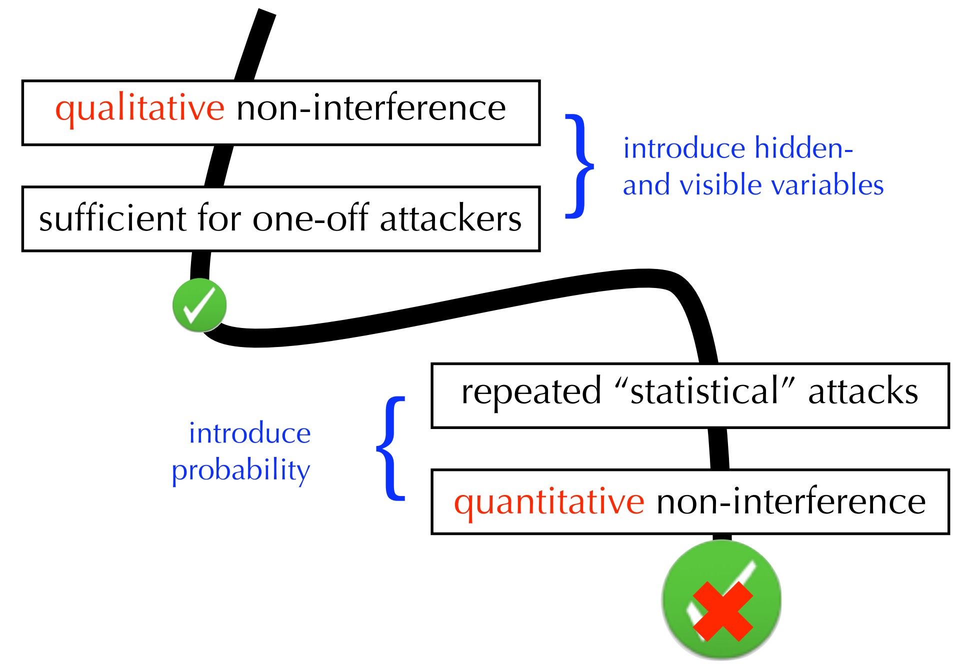
- Yet under repeated trials (in the café, rather than for just a one-off lunch date), the protocol is not secure unless the coins are fair.
- The only way *C* can say "I didn't pay" every single time is if *either* she always does *or* she never does (but we don't know which). In addition, the coins must be wholly fixed (but we don't know which way).
- Because we can learn this about *C,* if it is true and the coins are wholly fixed, then in that case it is leaking information. How then did we prove it correct without using fairness of the coins?

How does security lead to probability?

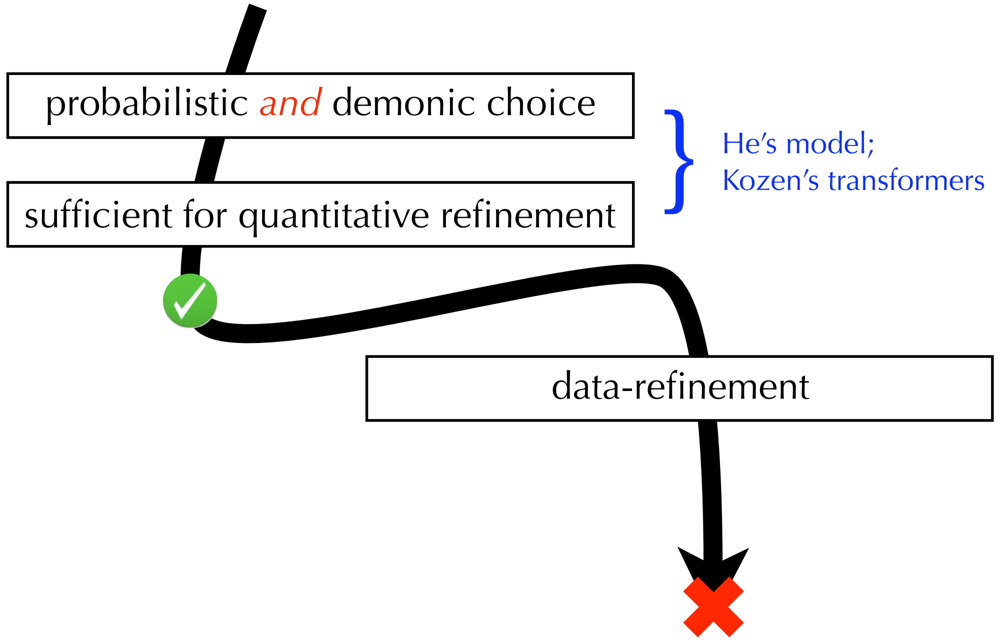


Goguen and Meseguer
Roscoe and Graham-Cumming
Leino and Joshi
Sabelfeld and Myers

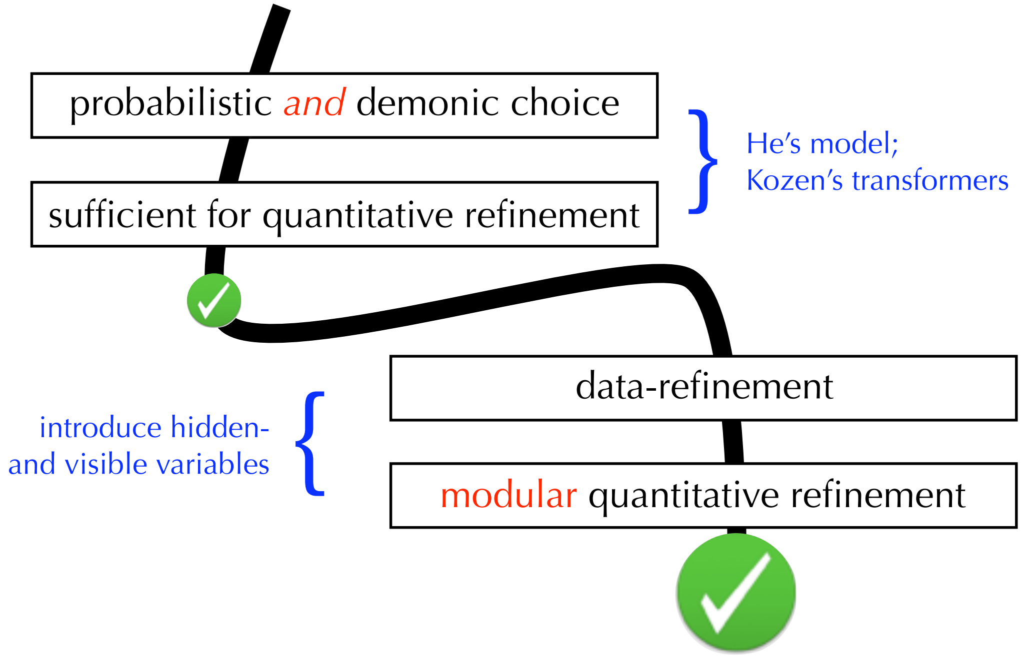
How does security lead to probability?

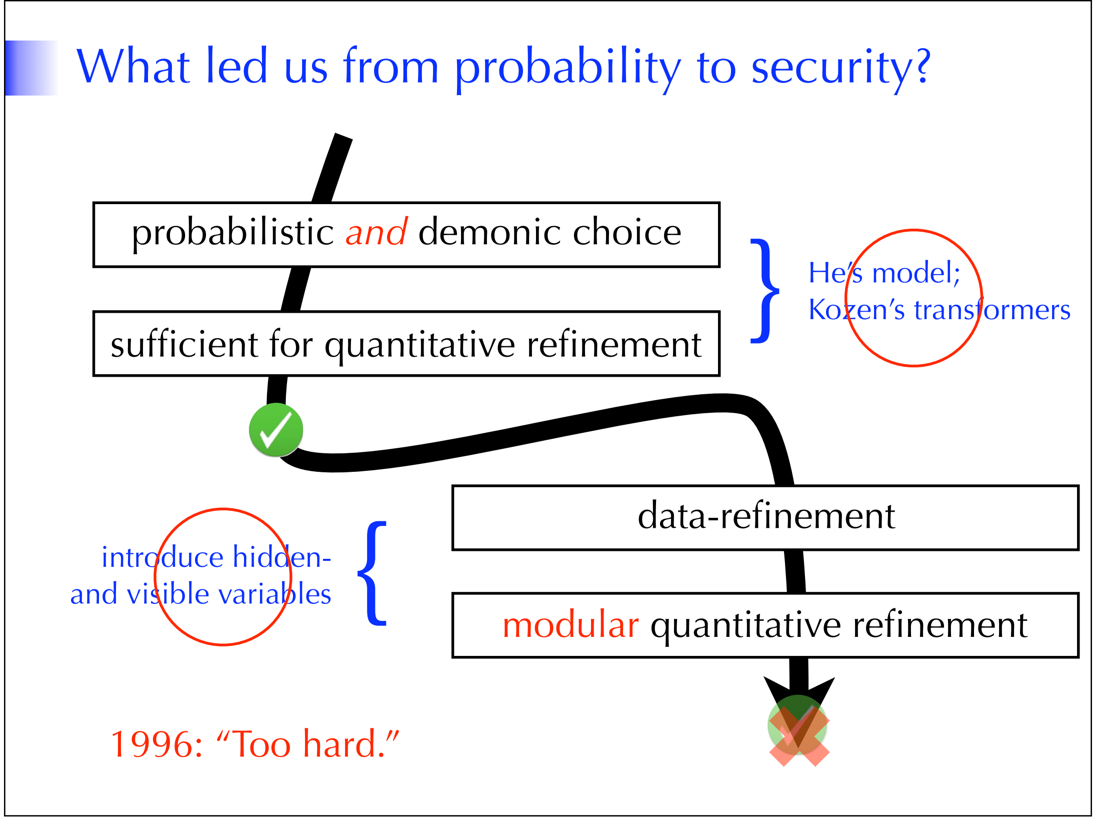


What led us from probability to security?



What led us from probability to security?




What led us from probability to security?
probabilistic and demonic choice
sufficient for quantitative refinement
He's model;
Kozen's transformers
data-refinement
introduce hidden-
and visible variables
modular quantitative refinement
1996: "Too hard."

What *exactly* is "too hard"?

- Purely demonic choice (without probability) has a perfectly adequate relational semantics.

- Purely probabilistic choice (without demons) is the subject of Markov Processes.

- Demonic and probabilistic choice together are modelled by Markov Decision Processes (MDP's): both He's model and (eg) Segala's are effectively this.

- Demonic choice, probabilistic choice and hiding are all three the topic of Partially Observable Markov Decision Processes (POMDP's).

What *exactly* is "too hard"?

- Purely demonic choice (without probability) has a perfectly adequate relational semantics.
- Purely probabilistic choice (without demons) is the subject of Markov Processes.
- Demonic and probabilistic choice together are modelled by Markov Decision Processes (MDP's): both He's model and (eg) Segala's are effectively this.
- Demonic choice, probabilistic choice and hiding are all three the topic of Partially Observable Markov Decision Processes (POMDP's).
- These theories are not "too hard" to understand.

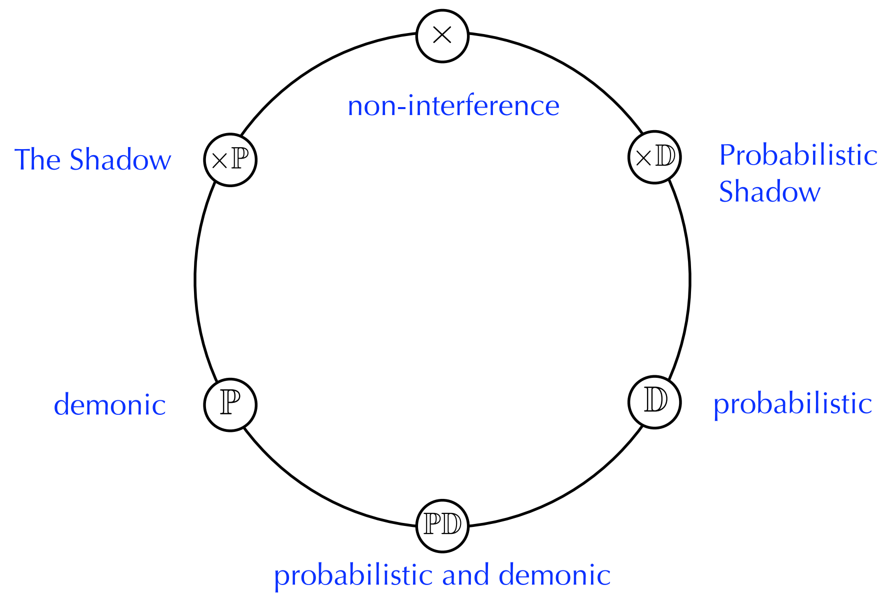
An important disclaimer

- The FM tools don't capture and make rigorous all the subjective criteria in the program's context. Often they make the requirements capture harder.
- The FM tools do not make it easier to prove mathematical facts than before. Often they make the proofs harder.
- The FM tools do make it easier to ensure that insights from the theory are accurately reflected in the structure of the program.
- The key in the design of FM tools is to find a formulation that unifies the algebra of the theory and the algebra of the programs/logic in a way that captures as much of both sides as is feasible.

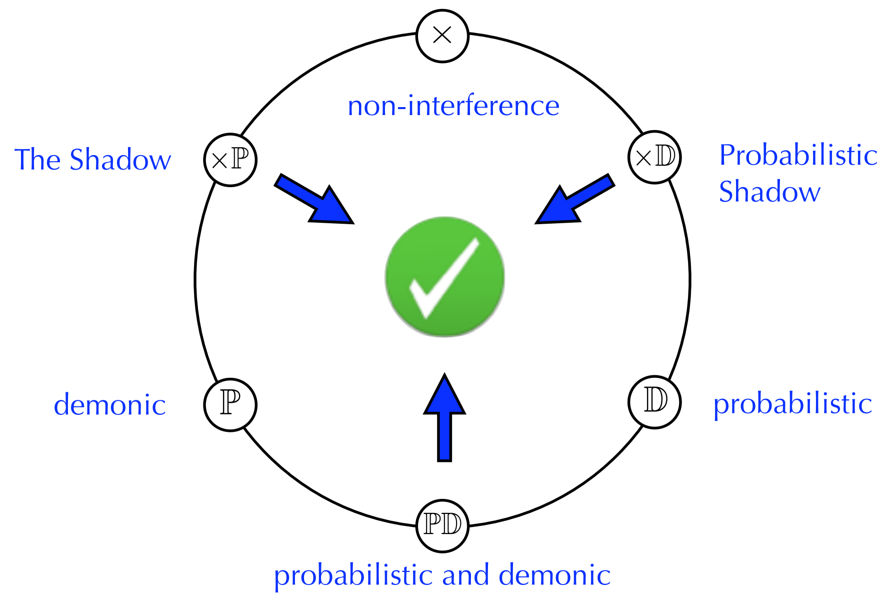
What *exactly* is "too hard"?

- Purely demonic choice (without probability) has a perfectly adequate relational semantics.
- Purely probabilistic choice (without demons) is the subject of Markov Processes.
- Demonic and probabilistic choice together are modelled by Markov Decision Processes (MDP's): both He's model and (eg) Segala's are effectively this.
- Demonic choice, probabilistic choice and hiding are all three the topic of Partially Observable Markov Decision Processes (POMDP's).
- That's why the *existence* of these theories is not in itself enough for Computer Science.

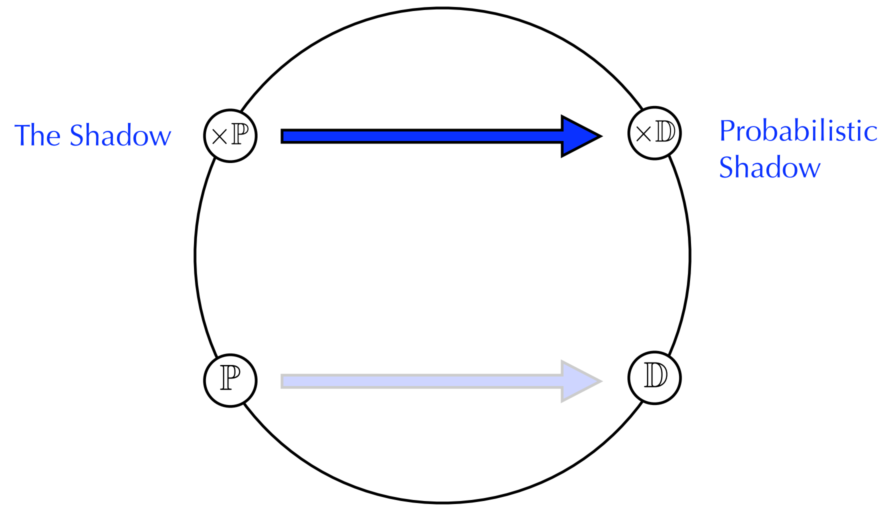
The many dimensions of probabilistic/ demonic models:



...we hope (ultimately) for this:



Meanwhile, let's design The Probabilistic Shadow



...and sort out The Café.

The (standard) Shadow: example

The semantics of shadow-enhanced programs is based on a division of the state-space S into visible- and hidden portions V and H, with programs' denotations then found in

$$V \times \mathbb{P}H \rightarrow \mathbb{P}(V \times \mathbb{P}H) \ .$$

We examine the two-statement program

$$h{:\in}\{0, 1, 2, 3\};\ v{:=}\, h \div 2$$

that chooses hidden h secretly from four possible values, and then –by assignment to visible v– reveals the more-significant bit.

The (standard) Shadow: example

$V \searrow \quad \swarrow \mathbb{P}H$

$(?, ?)$

$h :\in \{0, 1, 2, 3\};$

$v := h \div 2$

The (standard) Shadow: example

V $\quad\quad$ $\mathbb{P}H$

$(?, ?)$

$h{:\in}\,\{0,1,2,3\};$

$\{(?, \{0,1,2,3\})\}$ $\quad$ $\mathbb{P}(V \times \mathbb{P}H)$

$v{:=}\,h \div 2$

The (standard) Shadow: example

$$
\begin{array}{ll}
 & (?, ?) \\
 & h{:}\in \{0, 1, 2, 3\}; \\
\{ & (?, \{0, 1, 2, 3\}) \quad \} \\
 & v{:}= h \div 2
\end{array}
$$

$V \times \mathbb{P}H$

The (standard) Shadow: example

$$(?, ?)$$

$$h{:}\in \{0, 1, 2, 3\};$$

$$\{ \quad (?, \{0, 1, 2, 3\}) \quad \}$$

$$v{:=}\, h \div 2$$

$$\{(0, \{0, 1\}), (1, \{2, 3\})\}$$

$\mathbb{P}(V \times \mathbb{P}H)$

The (standard) Shadow: example

$$(?, ?)$$

$$h{:}\in \{0,1,2,3\};$$

$$\{ \quad (?, \{0,1,2,3\}) \quad \}$$

$\mathbb{P}(V \times \mathbb{P}H)$

$$v{:}= h \div 2$$

$$\{ \; \triangleright (0, \{0,1\}) \; , \quad \triangleright (1, \{2,3\}) \; \}$$

visible nondeterminism

The (standard) Shadow: example

$(?, ?)$

$h{:}\in \{0, 1, 2, 3\};$

$\{ \quad (?, \{0, 1, 2, 3\}) \quad \}$ — $\mathbb{P}(V \times \mathbb{P}H)$

$v{:=}\, h \div 2$

$\{ \quad (0, \{0, 1\}) \,,$

$\quad (1, \{2, 3\})$

$\}$

hidden nondeterminism

The probabilistic Shadow: example

The semantics of shadow-enhanced programs is based on a division of the state-space S into visible- and hidden portions V and H, with programs' denotations then found in

$$V \times \mathbb{D}H \rightarrow \mathbb{D}(V \times \mathbb{D}H) \ .$$

We examine the two-statement program

$$h{:}\in \{0^{@0.1}, 1^{@0.2}, 2^{@0.3}, 3^{@0.4}\}; \quad v{:=}\, h \div 2$$

that chooses hidden h secretly from four possible values, and then –by assignment to visible v– reveals the more-significant bit.

The probabilistic Shadow: example

V $\qquad$ $\mathbb{D}H$

$(?, ?)$

$h :\in \{0^{@0.1}, 1^{@0.2}, 2^{@0.3}, 3^{@0.4}\}$

$\{\ (?, \{0^{@0.1}, 1^{@0.2}, 2^{@0.3}, 3^{@0.4}\})^{@1}\ \}$

$v := h \div 2$

$\mathbb{D}(V \times \mathbb{D}H)$

The probabilistic Shadow: example

V $\qquad$ $\mathbb{D}H$

$(?, ?)$

$h{:\in}\,\{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\}$

$\{\ (?, \{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\})^{@1}\ \}$

$v{:=}\,h \div 2$

$\mathbb{D}(V \times \mathbb{D}H)$

The probabilistic Shadow: example

V $\quad$ $\mathbb{D}H$

$(?, ?)$

$h{:\in}\{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\}$

$\{\ (?, \{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\})^{@1}\ \}$

$v{:=}\,h \div 2$

$\mathbb{D}(V \times \mathbb{D}H)$

The probabilistic Shadow: example

$$(?, ?)$$

$$h :\in \{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\}$$

$$\{\quad (?, \{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\}) \quad {}^{@1}\}$$

$$v := h \div 2$$

The probabilistic Shadow: example

$$(?, ?)$$

$$h{:\in}\, \{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\}$$

$$\{\quad (?, \{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\}) \quad ^{@1}\}$$

$$v{:=}\, h \div 2$$

$$\{\quad (0, \{0^{@1/3},\ 1^{@2/3}\})\ ^{@0.3} \quad ,$$

$$(1, \{2^{@3/7},\ 3^{@4/7}\})\ ^{@0.7}$$

$$\}$$

The probabilistic Shadow: example

$$(?, ?)$$

$$h{:}\in \{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\}$$

$$\{\quad (?, \{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\})^{\quad @1}\}$$

$$v{:=}\, h \div 2$$

$$\{\quad (0, \{0^{@1/3},\ 1^{@2/3}\})^{\ @0.3}\ ,$$

$$(1, \{2^{@3/7},\ 3^{@4/7}\})^{\ @0.7}$$

$$\}$$

visible probability

The probabilistic Shadow: example

$$(?,?)$$

$$h{:\in}\,\{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\}$$

$$\{\quad (?,\{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\})\quad {}^{@1}\}$$

$$v{:=}\,h \div 2$$

$$\begin{array}{ll} \{ & (0,\{0^{@1/3},\ 1^{@2/3}\})\ ^{@0.3}\quad , \\ & (1,\{2^{@3/7},\ 3^{@4/7}\})\ ^{@0.7} \\ \} & \end{array}$$

hidden probability

The probabilistic Shadow: example

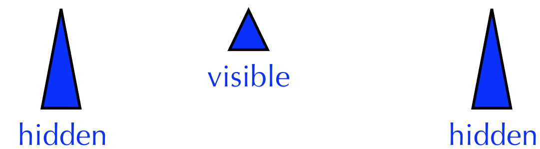
$$(?, ?)$$

$$h :\in \{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\}$$

$$\overline{(?, \{0^{@0.1},\ 1^{@0.2},\ 2^{@0.3},\ 3^{@0.4}\})}$$

$$v := h \div 2$$

$$(0, 0\ {}_{1/3}\!\oplus 1) \quad {}_{0.3}\!\oplus \quad (1, 2\ {}_{3/7}\!\oplus 3)$$



The (standard) Shadow: refinement

The standard Shadow extends (makes more restrictive) the usual relation of refinement that allows reduction of visible nondeterminism, so that e.g. we still have

$$\begin{array}{lccc} & v{:=}\,0 \sqcap v{:=}\,1 & \sqsubseteq & v{:=}\,0 \\ \text{and} & h{:=}\,0 \sqcap h{:=}\,1 & \sqsubseteq & h{:=}\,0 \end{array}$$

but we no longer have

$$h{:\in}\,\{0,1\} \quad \not\sqsubseteq \quad h{:=}\,0\ .$$

That's because in the last case the nondeterminism is *hidden* and cannot be reduced while maintaining an attacker's ignorance of h's possible values.

The probabilistic Shadow: refinement?

The probabilistic Shadow, on the other hand, has no "usual" notion of refinement to extend. That is, *purely probabilistic* assignments (while not wholly determined) have no non-trivial refinements: we note that

$$
\begin{array}{lccc}
 & v{:=}\,0 \;{}_p\!\oplus\; v{:=}\,1 & \not\sqsubseteq & v{:=}\,0 \;{}_q\!\oplus\; v{:=}\,1 \\
\text{and} & h{:=}\,0 \;{}_p\!\oplus\; h{:=}\,1 & \not\sqsubseteq & h{:=}\,0 \;{}_q\!\oplus\; h{:=}\,1 \;,
\end{array}
$$

unless of course $p{=}q$ — in which case it's equality anyway.

As with the standard Shadow, however, there is have a notion of *refinement of ignorance* — it's not present in the standard framework because ignorance cannot be expressed there. For the probabilistic Shadow this is the only kind of refinement.

``Amoeba'' refinement is present in both

In the standard Shadow, the refinement

$$h{:\in}\{0,1\} \sqcap h{:\in}\{1,2\} \quad \sqsubset \quad h{:\in}\{0,1,2\}$$

is strict, although it doesn't reduce the overall nondeterminism in h at all.

What it *does* reduce is an attacker's potential knowledge of h: on the left, he is certain to discover a final value that it cannot have (either it isn't 2 or it isn't 0).

On the right, however, he discovers nothing about h at all: that it's in $\{0,1,2\}$ he knows already.

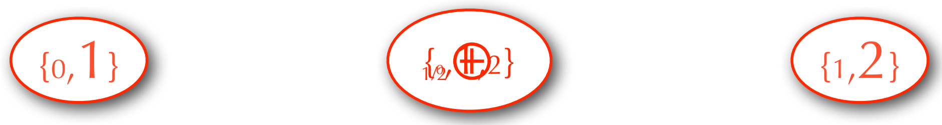
``Amoeba'' refinement is present in both

In the probabilistic Shadow, the refinement

$$
\begin{array}{ll}
 & h{:}\in \{0^{@2/3}, 1^{@1/3}\} \;\; {}_{1/2}\oplus \;\; h{:}\in \{1^{@1/3}, 2^{@2/3}\} \\
\sqsubset & h{:}\in \{0^{@1/3}, 1^{@1/3}, 2^{@1/3}\}
\end{array}
$$

is strict, although it doesn't change the *overall* final distribution of h at all.

What it *does* reduce is an attacker's likelihood of guessing the value of h: on the left, he will have a $2/3$ chance, once he's observed the resolution of the ${}_{1/2}\oplus$. On the right, his chance is at most $1/3$, no matter what he chooses.



The probabilistic Shadow: refinement?

This refinement over *structured distrib* corresponds to traditional formulations of entropy:

- (Conditional) Shannon Entropy increases up the refinement order;
- (Conditional) Guessing Entropy increases up the refinement order.

  (Expected number of guesses of the form “Is the secret C?” to achieve an affirmative answer.)

The probabilistic *Encryption Lemma*

$$
\begin{array}{ll}
& |[\ \mathbf{vis}\ v; \mathbf{hid}\ h'; \quad h' := 0\ {}_p\!\oplus 1;\ v := h + h'\ ]| \\
= & \text{“Atomicity lemma”} \\
& |[\ \mathbf{vis}\ v; \mathbf{hid}\ h'; \quad \langle\!\langle h' := 0\ {}_p\!\oplus 1;\ v := h + h' \rangle\!\rangle\ ]| \\
= & \text{“Classical reasoning”} \\
& |[\ \mathbf{vis}\ v; \mathbf{hid}\ h'; \quad \langle\!\langle v := h\ {}_p\!\oplus \neg h;\ h' := h + v \rangle\!\rangle\ ]| \\
= & \text{“Atomicity lemma”} \\
& |[\ \mathbf{vis}\ v; \mathbf{hid}\ h'; \quad v := h\ {}_p\!\oplus \neg h;\ h' := h + v\ ]| \\
= & \text{“Provided } p \text{ is } 1/2\text{”} \\
& |[\ \mathbf{vis}\ v; \mathbf{hid}\ h'; \quad v := 0\ {}_p\!\oplus 1;\ h' := h + v\ ]| \\
= & \text{“}h' \text{ is not free in } rhs \text{ of assignment to } v\text{”} \\
& |[\ \mathbf{vis}\ v;\ v := 0\ {}_p\!\oplus 1;\ |[\ \mathbf{hid}\ h';\ h' := h + v\ ]|\ ]| \\
= & \mathbf{skip}\ .
\end{array}
$$

The probabilistic *Encryption Lemma*

$$
\begin{array}{ll}
 & |[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad h' {:=} 0\ {}_p\!\oplus 1;\ \ v{:=}\, h{+}h'\ ]| \\
= & \text{“Atomicity lemma”} \\
 & |[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad \langle\!\langle h' {:=} 0\ {}_p\!\oplus 1;\ \ v{:=}\, h{+}h' \rangle\!\rangle\ ]| \\
= & \text{“Classical reasoning”} \\
 & |[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad \langle\!\langle v {:=} h\ {}_p\!\oplus \neg h;\ \ h'{:=}\, h{+}v \rangle\!\rangle\ ]| \\
= & \text{“Atomicity lemma”} \\
 & |[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad v {:=} h\ {}_p\!\oplus \neg h;\ \ h'{:=}\, h{+}v\ ]| \\
= & \text{“Provided } p \text{ is } 1/2\text{”} \\
 & |[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad v {:=} 0\ {}_p\!\oplus 1;\ \ h'{:=}\, h{+}v\ ]| \\
= & \text{“}h' \text{ is not free in } rhs \text{ of assignment to } v\text{”} \\
 & |[\ \textbf{vis}\ v;\ \ v {:=} 0\ {}_p\!\oplus 1;\ \ |[\ \textbf{hid}\ h';\ \ h'{:=}\, h{+}v\ ]|\,]| \\
= & \textbf{skip}\ .
\end{array}
$$

The probabilistic *Encryption Lemma*

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad h' := 0\ {}_p\!\oplus 1;\ v := h + h'\ ]|$$

$=$ "Atomicity lemma"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad \langle\!\langle h' := 0\ {}_p\!\oplus 1;\ v := h + h' \rangle\!\rangle\ ]|$$

$=$ "Classical reasoning"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad \langle\!\langle v := h\ {}_p\!\oplus \neg h;\ h' := h + v \rangle\!\rangle\ ]|$$

$=$ "Atomicity lemma"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad v := h\ {}_p\!\oplus \neg h;\ h' := h + v\ ]|$$

$=$ "Provided p is 1/2"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad v := 0\ {}_p\!\oplus 1;\ h' := h + v\ ]|$$

$=$ "h' is not free in rhs of assignment to v"

$$|[\ \textbf{vis}\ v;\ v := 0\ {}_p\!\oplus 1;\ |[\ \textbf{hid}\ h';\ h' := h + v\ ]|\ ]|$$

$=$ **skip** .

The probabilistic *Encryption Lemma*

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad h' := 0\ {}_p\!\oplus 1;\ v := h + h'\ ]|$$

$=$ "Atomicity lemma"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad \langle\!\langle h' := 0\ {}_p\!\oplus 1;\ v := h + h' \rangle\!\rangle\ ]|$$

$=$ "Classical reasoning"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad \langle\!\langle v := h\ {}_p\!\oplus \neg h;\ h' := h + v \rangle\!\rangle\ ]|$$

$=$ "Atomicity lemma"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad v := h\ {}_p\!\oplus \neg h;\ h' := h + v\ ]|$$

$=$ "Provided p is 1/2"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad v := 0\ {}_p\!\oplus 1;\ h' := h + v\ ]|$$

$=$ "h' is not free in *rhs* of assignment to v"

$$|[\ \textbf{vis}\ v;\ v := 0\ {}_p\!\oplus 1;\ |[\ \textbf{hid}\ h';\ h' := h + v\ ]|\ ]|$$

$=$ **skip** .

The probabilistic *Encryption Lemma*

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad h' := 0\ {}_p\!\oplus 1;\ \ v := h + h'\ ]|$$

$=$ "Atomicity lemma"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad \langle\!\langle h' := 0\ {}_p\!\oplus 1;\ \ v := h + h' \rangle\!\rangle\ ]|$$

$=$ "Classical reasoning"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad \langle\!\langle v := h\ {}_p\!\oplus \neg h;\ \ h' := h + v \rangle\!\rangle\ ]|$$

$=$ "Atomicity lemma"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad v := h\ {}_p\!\oplus \neg h;\ \ h' := h + v\ ]|$$

$=$ "Provided p is 1/2"

$$|[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad v := 0\ {}_p\!\oplus 1;\ \ h' := h + v\ ]|$$

$=$ "h' is not free in *rhs* of assignment to v"

$$|[\ \textbf{vis}\ v;\ \ v := 0\ {}_p\!\oplus 1;\ \ |[\ \textbf{hid}\ h';\ \ h' := h + v\ ]|\ ]|$$

$=$ **skip** .

The probabilistic *Encryption Lemma*

$$|[\ \mathbf{vis}\ v; \mathbf{hid}\ h';\quad h' := 0\ {}_p\!\oplus 1;\ v := h + h'\ ]|$$

= "Atomicity lemma"

$$|[\ \mathbf{vis}\ v; \mathbf{hid}\ h';\quad \langle\!\langle h' := 0\ {}_p\!\oplus 1;\ v := h + h' \rangle\!\rangle\ ]|$$

= "Classical reasoning"

$$|[\ \mathbf{vis}\ v; \mathbf{hid}\ h';\quad \langle\!\langle v := h\ {}_p\!\oplus \neg h;\ h' := h + v \rangle\!\rangle\ ]|$$

= "Atomicity lemma"

$$|[\ \mathbf{vis}\ v; \mathbf{hid}\ h';\quad v := h\ {}_p\!\oplus \neg h;\ h' := h + v\ ]|$$

= "Provided p is $1/2$"

$$|[\ \mathbf{vis}\ v; \mathbf{hid}\ h';\quad v := 0\ {}_p\!\oplus 1;\ h' := h + v\ ]|$$

= "h' is not free in *rhs* of assignment to v"

$$|[\ \mathbf{vis}\ v;\ v := 0\ {}_p\!\oplus 1;\ |[\ \mathbf{hid}\ h';\ h' := h + v\ ]|\ ]|$$

= **skip** .

The probabilistic *Encryption Lemma*

$$\begin{array}{ll}
& |[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad h' := 0\ {}_p\!\oplus\ 1;\ \ v := h + h'\ ]| \\
= & \text{“Atomicity lemma”} \\
& |[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad \langle\!\langle h' := 0\ {}_p\!\oplus\ 1;\ \ v := h + h' \rangle\!\rangle\ ]| \\
= & \text{“Classical reasoning”} \\
& |[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad \langle\!\langle v := h\ {}_p\!\oplus\ \neg h;\ \ h' := h + v \rangle\!\rangle\ ]| \\
= & \text{“Atomicity lemma”} \\
& |[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad v := h\ {}_p\!\oplus\ \neg h;\ \ h' := h + v\ ]| \\
= & \text{“Provided } p \text{ is } 1/2\text{”} \\
& |[\ \textbf{vis}\ v; \textbf{hid}\ h';\quad v := 0\ {}_p\!\oplus\ 1;\ \ h' := h + v\ ]| \\
= & \text{“} h' \text{ is not free in } \textit{rhs} \text{ of assignment to } v\text{”} \\
& |[\ \textbf{vis}\ v;\ \ v := 0\ {}_p\!\oplus\ 1;\ \ |[\ \textbf{hid}\ h';\ \ h' := h + v\ ]|\ ]| \\
= & \textbf{skip}\ .
\end{array}$$

The probabilistic *Encryption Lemma*

$$
\begin{array}{ll}
& |[\ \mathbf{vis}\ v; \mathbf{hid}\ h'; \quad h' := 0\ {}_{1/2}{\oplus}\ 1;\ \ v := h + h'\ ]| \\
= & \text{“Atomicity lemma”} \\
& |[\ \mathbf{vis}\ v; \mathbf{hid}\ h'; \quad \langle\!\langle h' := 0\ {}_{1/2}{\oplus}\ 1;\ \ v := h + h' \rangle\!\rangle\ ]| \\
= & \text{“Classical reasoning”} \\
& |[\ \mathbf{vis}\ v; \mathbf{hid}\ h'; \quad \langle\!\langle v := h\ {}_{1/2}{\oplus}\ \neg h;\ \ h' := h + v \rangle\!\rangle\ ]| \\
= & \text{“Atomicity lemma”} \\
& |[\ \mathbf{vis}\ v; \mathbf{hid}\ h'; \quad v := h\ {}_{1/2}{\oplus}\ \neg h;\ \ h' := h + v\ ]| \\
= & \text{“Symmetry”} \\
& |[\ \mathbf{vis}\ v; \mathbf{hid}\ h'; \quad v := 0\ {}_{1/2}{\oplus}\ 1;\ \ h' := h + v\ ]| \\
= & \text{“}h' \text{ is not free in } rhs \text{ of assignment to } v\text{”} \\
& |[\ \mathbf{vis}\ v;\ \ v := 0\ {}_{1/2}{\oplus}\ 1;\ \ |[\ \mathbf{hid}\ h';\ \ h' := h + v\ ]|\,]| \\
= & \mathbf{skip}\ .
\end{array}
$$

The standard *Encryption Lemma*

$$|[\ \mathbf{vis}\ v; \mathbf{hid}\ h';\quad h' {:\in} \{0,1\}\quad ;\ v{:=}h{+}h'\ ]|$$

• The Dining Cryptographers	Maths. Prog. Const. vi2006
• Rivest's Oblivious Transfer	Sci. Comp. Prog. i2009
• The 1001 Cryptographers	CARH Festschrift article iii2009
• The Three Judges	CARH Festschrift presentation iv2009
• Secure Database Lookup	ICTAC vi2009
• The Millionaires	FM xi2009

$$=\quad \mathbf{skip}\ .$$

The standard *Encryption Lemma*

$$|[\ \mathbf{vis}\ v; \mathbf{hid}\ h';\quad h' :\in \{0,1\}\quad ;\ v := h + h'\ ]|$$

•	The Dining Cryptographers	Maths. Prog. Const. vi2006	✖
•	Rivest's Oblivious Transfer	Sci. Comp. Prog. i2009	✖
•	The 1001 Cryptographers	CARH Festschrift article iii2009	✖
•	The Three Judges	CARH Festschrift presentation iv2009	✖
•	Secure Database Lookup	ICTAC vi2009	✖
•	The Millionaires	FM xi2009	✖

$= \ \mathbf{skip}\ .$

Sound for one-off's — but not for the café

The probabilistic *Encryption Lemma*

$$|[\ \mathbf{vis}\ v; \mathbf{hid}\ h';\ h' := 0\ {}_{1/2}\oplus\ 1;\ v := h + h'\ ]|$$

- The Dining Cryptographers — Maths. Prog. Const. vi2006 ✓
- Rivest's Oblivious Transfer — Sci. Comp. Prog. i2009 ✓
- The 1001 Cryptographers — CARH Festschrift article iii2009 ✓
- The Three Judges — CARH Festschrift presentation iv2009 ✓
- Secure Database Lookup — ICTAC vi2009 ✓
- The Millionaires — FM xi2009 ✓

$$=\ \ \mathbf{skip}\ .$$

Café-Certified: and proofs unchanged.