Way below security

Dusko Pavlovic

Kestrel Institute and OUCL

April 2009

MFPS XXV, Oxford

Session honoring Mike Mislove

Outline

Outline

Security and domains?

Information systems, honesty, and guards

Domains for Bayesian inference and guessing

Summary

Security is complicated

Crypto system

Given the types

- $\mathcal{M}$ of *plaintexts*
- $\mathcal{C}$ of *cyphertexts*
- $\mathcal{K}$ of *keys*
- $\mathcal{R}$ of *random seeds*

Security is complicated

Crypto system

Given the types

- $\mathcal{M}$ of *plaintexts*
- $\mathcal{C}$ of *cyphertexts*
- $\mathcal{K}$ of *keys*
- $\mathcal{R}$ of *random seeds*

a *crypto-system* is a triple of algorithms:

- key generation $\langle k, \overline{k} \rangle : \mathcal{R} \longrightarrow \mathcal{K} \times \mathcal{K}$,
- encryption $\mathsf{E} : \mathcal{R} \times \mathcal{K} \times \mathcal{M} \longrightarrow \mathcal{C}$, and
- decryption $\mathsf{D} : \mathcal{K} \times \mathcal{C} \longrightarrow \mathcal{M}$,

Security is complicated

Crypto system

. . . that together provide

- unique decryption:

$$\mathsf{D}(\overline{k}, \mathsf{E}(k, m)) \quad = \quad m$$

Security is complicated

Crypto system

...that together provide

- unique decryption:

$$D(\overline{k}, E(k, m)) \quad = \quad m$$

- secrecy (IND-CCA):

$$\mathrm{Prob}\left(\begin{array}{l} c_0 \in \mathbb{A}_0,\ m = D(\overline{k}, c_0), \\ m_0, m_1 \in \mathbb{A}_1(c_0, m), c \in E(k, m_b) \\ c_1 \in \mathbb{A}_2(c_0, m, m_0, m_1, c^{\neq}), \widetilde{m} = D(\overline{k}, c_1) \end{array} \quad \vdash \quad b \in \mathbb{A}_3(c_0, m, m_0, m_1, c, c_1, \widetilde{m}) \right) \quad \leq \quad \frac{1}{2}$$

for any probabilistic algorithm $\mathbb{A} = \langle \mathbb{A}_0, \mathbb{A}_1, \mathbb{A}_2, \mathbb{A}_3 \rangle$

Idea

Symbolically, the secret is guarded by a key

$$\forall \Theta. \quad \Theta,\ \mathsf{E}(k,m) \vdash m \quad \Longrightarrow \quad \Theta \vdash k$$

$$\Updownarrow$$

$$k \quad \text{guards} \quad m \quad \text{in} \quad \mathsf{E}(k,m)$$

Idea

Symbolically, the secret is guarded by a key

$$\forall \Theta. \quad \Theta,\ \mathsf{E}(k,m) \vdash m \quad \Longrightarrow \quad \Theta \vdash k$$

$$\Updownarrow$$

$$k \quad \text{guards} \quad m \quad \text{in} \quad \mathsf{E}(k,m)$$

Does that mean that the key is way-below the secret?

$$\forall J. \quad \bigsqcup J \sqsupseteq m \quad \Longrightarrow \quad J \sqsupseteq k$$

$$\Updownarrow$$

$$k \quad \ll \quad m$$

Outline

Information system of a protocol

Algebraic model

- algebra $\mathbb{T}$
  - equational presentation (Σ, E), generators V
- principals $\mathcal{W}$
  - $A \in \mathcal{W}$ owns $x \in \mathrm{V}_A$, a store, nonce or key
- fixed protocol run $\mathcal{Q}$
  - $A \in \mathcal{W}$ may send $t \in \mathbb{T}$, or receive into $x \in \mathrm{V}_A$

Information system of a protocol

Derivability

$$\Gamma \vdash \Theta \iff \forall t \in \Theta \;\; \exists \varphi \in \Sigma^* \;\; \exists \vec{g} \subseteq \Gamma. \;\; \varphi(\vec{g}) \stackrel{E}{=} t$$

Consistent sets

$$\Gamma_A^{\mathcal{Q}} = A\text{'s environment in } \mathcal{Q}$$

$$\mathsf{Con}_A^{\mathcal{Q}} = \{\Theta \in \wp_{fin}\mathbb{T} \mid \Gamma_A^{\mathcal{Q}} \vdash \Theta\}$$

$$\mathsf{Con}^{\mathcal{Q}} = \bigcup_{A \in \mathcal{W}} \mathsf{Con}_A^{\mathcal{Q}}$$

Example: Encryption protocol

- $\Sigma = \{\mathsf{E}, \mathsf{D} : \mathbb{T} \times \mathbb{T} \longrightarrow \mathbb{T}\}$
- $E = \{\mathsf{D}(x, \mathsf{E}(x, y)) = y\}$
- $\mathcal{Q} = \{A \xrightarrow{\mathsf{E}(k,m)} B\}$
  - $k \in \Gamma_X \iff X \in \{A, B\}$
  - $m \in \Gamma_X \iff X = A$

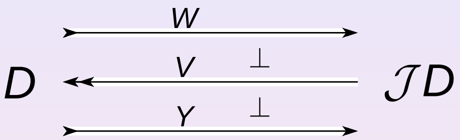
Domain of a protocol

$$D^{\mathcal{Q}} = \{a \in \wp\mathbb{T} \mid \forall \Theta \underset{fin}{\subseteq} a.\ \Theta \in \mathsf{Con}^{\mathcal{Q}} \wedge \Theta \vdash \Gamma \Rightarrow \Gamma \subseteq a\}$$

Order ideals

$$\mathcal{J}D \;=\; \Big\{ J \in D \;\;\big|\;\; \forall a \subseteq b \in J \Rightarrow a \in J \\ \wedge\;\; \forall ab \in J\ \exists c \in J.\ a, b \subseteq c \Big\}$$

Continuity = left adjoint to $\bigsqcup$



$$
\begin{aligned}
Y(a) &= \{x \sqsubseteq a\} \\
V(J) &= \bigsqcup J \\
W(a) &= \{x \ll a\}
\end{aligned}
$$

Continuity = left adjoint to $\bigsqcup$

Intuition

- $W(a) = \{x \ll a\}$ are the *key elements* of a
  - if $\bigsqcup J \sqsupseteq a$ is a "computation" of a
  - then $k \ll a$ means $k \in J$ for every such computation.
- $VW(a) = a$ means that a can be computed from its key elements.

Example: Encryption protocol

- $W(m) = \{m\}$

Example: Encryption protocol

- $W(m) = \{m\}$:(

Example: Encryption protocol

- $W(m) = \{m\}$:(
  - although m is never sent in the clear
  - and no principal knows it without k

Example: Encryption protocol

- $W(m) = \{m\}$:(
  - although m is never sent in the clear
  - and no principal knows it without k
- $\mathrm{Con}^{\mathcal{Q}}$ contains some sets that never occur
  - they cover the honesty assumptions

Example: Encryption protocol

- $W(m) = \{m\}$:(
  - although m is never sent in the clear
  - and no principal knows it without k
- $\mathrm{Con}^{\mathcal{Q}}$ contains some sets that never occur
  - they cover the honesty assumptions
- culprit: $\forall a \subseteq b \in J \Rightarrow a \in J$
  - every derivable term is derivable on its own

Honesty system of a protocol

Derivability

$$\Gamma \vdash \Theta \iff \forall t \in \Theta \;\; \exists \varphi \in \Sigma^* \;\; \exists \vec{g} \subseteq \Gamma. \;\; \varphi(g) \stackrel{E}{=} t$$

Honest sets

$$\begin{aligned}
\Gamma_A^{\mathcal{Q}} &= A\text{'s environment in } \mathcal{Q} \\
\mathrm{Hon}_A^{\mathcal{Q}} &= \{\Theta \in \wp_{fin}\mathbb{T} \mid \Gamma_A^{\mathcal{Q}} \subseteq \Theta \wedge \Gamma_A^{\mathcal{Q}} \vdash \Theta\} \\
\mathrm{Hon}^{\mathcal{Q}} &= \bigcup_{A \in \mathcal{W}} \mathrm{Hon}_A^{\mathcal{Q}}
\end{aligned}$$

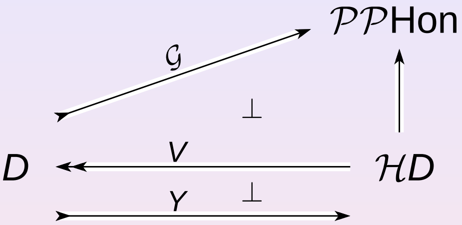
Domain of a protocol

$$D^{\mathcal{Q}} = \{a \in \wp\mathbb{T} \mid \forall \Xi \underset{fin}{\subseteq} a\ \exists \Theta \in \mathsf{Hon}^{\mathcal{Q}}.\ \Xi \subseteq \Theta \wedge \Xi \vdash \Gamma \Rightarrow \Gamma \subseteq a\}$$

Honest ideals

$$\mathcal{H}D = \Big\{ H \in D \;\Big|\; \forall a \subseteq b \in H$$
$$(\exists \Theta \in \mathrm{Hon}.\ \Theta \subseteq a) \Rightarrow a \in H$$
$$\wedge\ \forall ab \in H\ \exists c \in H.\ a, b \subseteq c \Big\}$$

Guards = left multi-adjoint to $\bigsqcup$

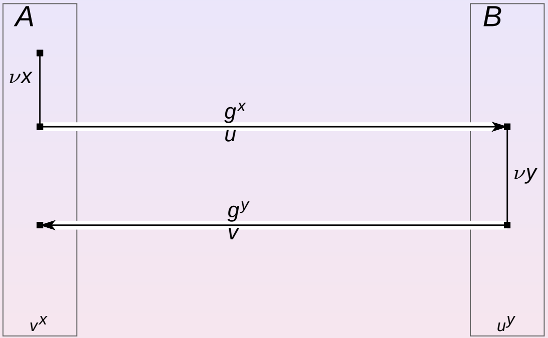


$$a \sqsubseteq V(H) \iff \exists G \in \mathcal{G}(a).\ G \sqsubseteq H$$

Example: Encryption protocol

- $\mathcal{G}(m) = \{\{k\}\}$:)

Example: Diffie-Hellman Key Agreement



Example: Diffie-Hellman Key Agreement

- $W(g^{xy}) = \{g^{xy}\}$:(
- $\mathcal{G}(g^{xy}) = \{\{g^x, y\}, \{g^y, x\}\}$:)

Algebraic theory of secrecy

(Meadows & DP)

$$\mathcal{G} \ \text{guards}_{\Upsilon}\Theta \quad = \quad \forall t \in \Theta\ \forall \Xi \subseteq \Upsilon\ \exists \Gamma \in \mathcal{G}.\ \Xi \vdash t \Rightarrow \Xi \vdash \Gamma$$

Algebraic theory of secrecy

(Meadows & DP)

$$\begin{aligned}
\mathsf{Have}(\Theta; G) &= \forall X \in G.\ \Gamma_X \vdash \Theta \\
\mathsf{Only}(\Theta; G) &= \forall X \in \mathcal{W}\ \forall t \in \Theta.\ \Gamma_X \vdash t \Rightarrow X \in G \\
\mathsf{Secr}(\Theta; G) &= \mathsf{Have}(\Theta; G) \wedge \mathsf{Only}(\Theta; G) \\
&= \forall X \in \mathcal{W}\ \forall t \in \Theta.\ \Gamma_X \vdash t \Leftrightarrow X \in G
\end{aligned}$$

Algebraic theory of secrecy

(Meadows & DP)

$$\frac{\mathrm{Have}(\Xi; G) \qquad \Xi \vdash_G \Theta}{\mathrm{Have}(\Theta; G)}$$

$$\frac{\mathrm{Only}(\Xi_i; G_i)\ \Big|_{i=1}^{n} \qquad \{\Xi_i\}_{i=1}^{n} \text{ guards } \Theta}{\mathrm{Only}(\Theta; \bigcup_{i=1}^{n} G_i)}$$

$$\frac{\mathrm{Secr}(\Xi_i; G_i)\ \Big|_{i=1}^{n} \quad \Xi_i \vdash_{G_i} \Theta\ \Big|_{i=1}^{n} \quad \{\Xi_i\}_{i=1}^{n} \text{ guards } \Theta}{\mathrm{Secr}(\Theta; \bigcup_{i=1}^{n} G_i)}$$

Security is complicated

Crypto system

- unique decryption:

$$\mathsf{D}(\overline{k}, \mathsf{E}(k, m)) \quad = \quad m$$

- secrecy (IND-CCA):

$$\mathrm{Prob}\left(\begin{array}{l} c_0 \in \mathbb{A}_0,\ m = \mathsf{D}(\overline{k}, c_0), \\ m_0, m_1 \in \mathbb{A}_1(c_0, m), c \in \mathsf{E}(k, m_b) \\ c_1 \in \mathbb{A}_2(c_0, m, m_0, m_1, c^{\neq}), \widetilde{m} = \mathsf{D}(\overline{k}, c_1) \end{array} \quad \vdash \quad b \in \mathbb{A}_3(c_0, m, m_0, m_1, c, c_1, \widetilde{m}) \right) \quad \leq \quad \frac{1}{2}$$

for any probabilistic algorithm $\mathbb{A} = \langle \mathbb{A}_0, \mathbb{A}_1, \mathbb{A}_2, \mathbb{A}_3 \rangle$

Outline

Idea

- assume that the algebra $\mathbb{T}$ is given with
  - an implementation

$$\begin{aligned} [\![-]\!] &: \mathcal{T} \to \mathcal{L} \\ \surd &: \mathcal{L} \rightharpoonup \mathcal{T} \end{aligned}$$

    such that $\surd [\![t]\!] = t$

  - monoid of feasible maps $\mathcal{F} \subseteq \mathcal{L}^{\mathcal{L}}$
  - frequency distribution

$$\mathsf{Prob} \ : \ \mathbb{T} \longrightarrow [0,1]$$

Idea

- generalize
  - from algebraic derivability

$$\begin{array}{rccc} - \vdash - \ : & D \times D & \longrightarrow & \{0,1\} \\ & \Gamma, \Theta & \longmapsto & \Gamma \vdash \Theta \end{array}$$

  - to Bayesian inference

$$\begin{array}{rccc} (- \vdash -) \ : & D \times D & \longrightarrow & [0,1] \\ & \Gamma, \Theta & \longmapsto & \mathrm{Prob}\,(\Gamma \vdash \Theta) \end{array}$$

  - and guessing (cryptanalysis)

$$\begin{array}{rccc} [- \vdash -] \ : & D \times D & \longrightarrow & [0,1] \\ & \Gamma, \Theta & \longmapsto & \bigvee_{\mathbb{A} \in \mathcal{F}} \mathrm{Prob}\,(\Gamma \vdash \Theta \in \mathbb{A}(\Gamma)) \end{array}$$

Hope

Develop

- a manageable formalization of guessing
- using information systems
- *enriched* over the ordered monoid $\left([0,1],\ \cdot,\ 1,\ \leq\ \right)$
- treat $\left(\Gamma \vdash \Theta\right)$ and $\left[\Gamma \vdash \Theta\right]$ as hom-objects in $[0,1]$
  - the states $\Gamma, \Theta \ldots$ can now be viewed as sets of equations *and inequalities*

Problem

The Bayesian inference and guessing are **not** transitive:

$$\left(\Xi \vdash \Gamma\right)\cdot\left(\Gamma \vdash \Theta\right) \quad \not\leq \quad \left(\Xi \vdash \Theta\right)$$
$$\left[\Xi \vdash \Gamma\right]\cdot\left[\Gamma \vdash \Theta\right] \quad \not\leq \quad \left[\Xi \vdash \Theta\right]$$

Problem

The Bayesian inference and guessing are **not** transitive:

$$(\Xi \vdash \Gamma)\cdot(\Gamma \vdash \Theta) \quad \not\leq \quad (\Xi \vdash \Theta)$$
$$[\Xi \vdash \Gamma]\cdot[\Gamma \vdash \Theta] \quad \not\leq \quad [\Xi \vdash \Theta]$$

e.g., for

- $\Gamma = \emptyset$, thus $(\Xi \wedge \Gamma) = (\Xi)$
  - $(\Xi \vdash \Gamma) = \frac{(\Xi \wedge \Gamma)}{(\Xi)} = 1$
- $\Theta = \neg\Xi$
  - $(\Gamma \vdash \Theta) = (\emptyset \vdash \neg\Xi) = 1 - (\Xi)$
  - $(\Xi \vdash \Theta) = \frac{(\Xi \wedge \neg\Xi)}{(\Xi)} = 0$

Problem

…but they do satisfy

$$(\Xi \vdash \Gamma)\cdot(\Xi,\Gamma \vdash \Theta) \;=\; (\Xi \vdash \Gamma,\Theta)$$
$$[\Xi \vdash \Gamma]\cdot[\Xi,\Gamma \vdash \Theta] \;=\; [\Xi \vdash \Gamma,\Theta]$$

because

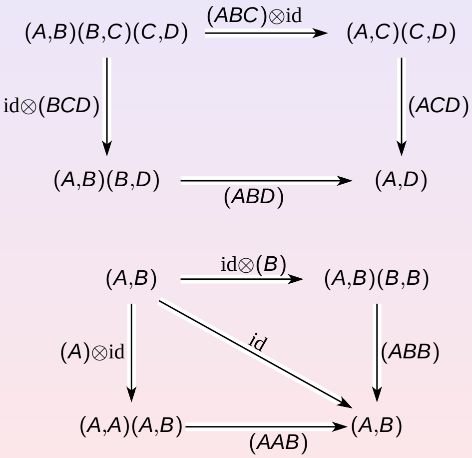
$$\frac{(\Xi\Gamma)}{(\Xi)}\cdot\frac{(\Xi\Gamma\Theta)}{(\Xi\Gamma)} \;=\; \frac{(\Xi\Gamma\Theta)}{(\Xi)}$$

$\mathbb{V}$-categories

- $(\mathbb{V}, \otimes, I)$
  - monoidal category, abbreviate $k \otimes \ell$ to $k\ell$
- $\mathbb{C} = \{A, B, \ldots\}$
  - class of objects
- $(A, B) \in \mathbb{V}$
  - hom-objects, for every $A, B \in \mathbb{C}$
- $(ABC) : (A, B) \otimes (B, C) \longrightarrow (A, C)$
  - composition, for every $A, B, C \in \mathbb{C}$
- $(A) : I \longrightarrow (A, A)$
  - identities, for every $A \in \mathbb{C}$

$\mathbb{V}$-categories

... satisfying



$\mathbb{V}$-categories

Examples

- $\mathbb{V} = \left(\{0,1\}, \wedge, 1\right)$ — preorders
- $\mathbb{V} = \left(\mathsf{Set}, \times, 1\right)$ — categories
- $\mathbb{V} = \left([0,\infty], +, 0\right)$ — metric spaces

$\mathbb{V}$-dependencies

- $(\mathbb{V}, \otimes, I)$
  - monoidal category, abbreviate $k \otimes \ell$ to $k\ell$
- $(\mathbb{C}, \cdot, \top)$
  - abelian monoid of objects, abbreviate $A \cdot B$ to AB
- $(A, B) \in \mathbb{V}$
  - hom-objects, for every $A, B \in \mathbb{C}$
- $(ABC) : (A, B) \otimes (AB, C) \longrightarrow (A, BC)$
  - composition, for every $A, B, C \in \mathbb{C}$
- $\pi(AB) : I \longrightarrow (AB, B)$ and
  $\delta(AB) : (A, B) \longrightarrow (A, BB)$
  - projections and diagonals, for every $A, B \in \mathbb{C}$

$\mathbb{V}$-dependencies

...satisfying

$$
\begin{array}{ccc}
(A,B)(AB,C)(ABC,D) & \xrightarrow{(ABC)\otimes \mathrm{id}} & (A,BC)(ABC,D) \\
{\scriptstyle \mathrm{id}\otimes((AB)CD)}\big\downarrow & & \big\downarrow{\scriptstyle (A(BC)D)} \\
(A,B)(AB,CD) & \xrightarrow[(AB(CD))]{} & (A,BCD)
\end{array}
$$

$$
\begin{array}{ccc}
(A,B) & & \\
{\scriptstyle \pi(A\top)\otimes \mathrm{id}}\big\downarrow & \searrow^{\mathrm{id}} & \\
(A,\top)(A,B) & \xrightarrow[(A\top B)]{} & (A,B)
\end{array}
\qquad
\begin{array}{ccc}
(A,B) & \xrightarrow{\mathrm{id}\otimes\pi(AB)} & (A,B)(AB,B) \\
 & \searrow^{\delta(AB)} & \big\downarrow{\scriptstyle (ABB)} \\
 & & (A,BB)
\end{array}
$$

$\mathbb{V}$-dependencies

Examples

- $\mathbb{V} = (\{0,1\}, \wedge, 1)$ — semilattices

$$a \leq b \wedge ab \leq c \iff a \leq bc$$

- $\mathbb{V} = (\mathrm{Set}, \times, 1)$ — dependent types (RCCCs)

$$\begin{array}{rrcl} & (x:A & \rhd & f(x) : B(x)) \\ \times & (x:A, y:B(x) & \rhd & g(x,y) : C(x,y)) \\ \longrightarrow & (x:A & \rhd & \langle f(x), g(x,f(x))\rangle : B(x) \times C(x,f(x))) \end{array}$$

- $\mathbb{V} = ([0,1], \cdot, 1)$ — Bayesian nets

$$(A \vdash B) \cdot (AB \vdash C) = (A \vdash BC)$$

Domain theory of Bayesian inference

Definition

Let $\mathbb{D}$ be a $[0,1]$-dependency. A *Bayesian ideal* is a map $\varphi : \mathbb{D} \longrightarrow [0,1]$ such that

$$(\Xi \vdash \Theta) \cdot \varphi(\Xi\Theta) \quad \leq \quad \varphi(\Xi)$$

We denote by $\mathcal{J}\mathbb{D}$ the dependency of Bayesian ideals, with the monoid and hom-object structure

$$\begin{aligned} \varphi \cdot \psi(\Theta) &= \varphi(\Theta) \cdot \psi(\Theta) \\ (\varphi \vdash \psi) &= \bigwedge_{\Theta \in \mathbb{D}} \left(\frac{\varphi(\Theta)}{\psi(\Theta)} \wedge \frac{\psi(\Theta)}{\varphi(\Theta)} \right) \end{aligned}$$

Domain theory of guessing

Definition

Let $\mathbb{D}$ be a $[0,1]$-dependency. A *guessing ideal* is an algorithm $\Phi : \mathbb{D} \longrightarrow [0,1]$ such that

$$\left[\Xi \vdash \Theta\right]\cdot\Phi(\Xi\Theta) \quad \leq \quad \Phi(\Xi)$$

We denote by $\mathcal{H}\mathbb{D}$ the dependency of guessing ideals, with the monoid and hom-object structure

$$\begin{aligned}\Phi\cdot\Psi(\Theta) \quad &= \quad \Phi(\Theta)\cdot\Psi(\Theta)\\ \left[\Phi \vdash \Psi\right] \quad &= \quad \bigwedge_{\Theta\in\mathbb{D}}\left(\frac{\Phi(\Theta)}{\Psi(\Theta)} \wedge \frac{\Psi(\Theta)}{\Phi(\Theta)}\right)\end{aligned}$$

Ideals are Cauchy sequences

Theorem

Bayesian (resp. guessing) ideals over a $[0,1]$*-dependency* $\mathbb{D}$ *correspond to the sequences of events (resp. guesses)* $\langle \Theta_i \rangle_{i=1}^{\infty}$ *such that*

$$\forall k \in \mathbb{N}\ \exists N \in \mathbb{N}\ \forall n > N\ \forall m \in \mathbb{N}.$$
$$\left(\Theta_1, \Theta_2, \ldots, \Theta_n \vdash \Theta_{n+m}\right) \quad \geq \quad e^{-\frac{1}{k}}$$

$$\exists N \in \mathcal{F}\ \forall k \in \mathbb{N}\ \forall n > N(k)\ \forall m \in \mathbb{N}.$$
$$\left[\Theta_1, \Theta_2, \ldots, \Theta_n \vdash \Theta_{n+m}\right] \quad \geq \quad e^{-\frac{1}{k}}$$

Guessing by adjoints

Fact.

$$\mathbb{D} \xrightarrow{Y} \mathcal{H}\mathbb{D}$$

$$Y(\Theta) = [- \vdash \Theta]$$

Guessing by adjoints

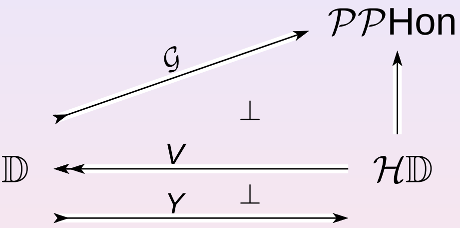
Proposition

$$\mathbb{D} \underset{Y}{\overset{V}{\twoheadleftarrow\!\!\!\rightarrowtail}} \mathcal{H}\mathbb{D} \qquad (V \dashv Y:\ V : \mathcal{H}\mathbb{D} \twoheadrightarrow \mathbb{D},\ Y : \mathbb{D} \rightarrowtail \mathcal{H}\mathbb{D},\ \bot)$$

$$\begin{aligned} Y(\Theta) &= [- \vdash \Theta] \\ V(\Theta_i) &= \lim_{i \to \infty} \Theta_i \end{aligned}$$

Guessing by adjoints

Proposition



$$
\begin{aligned}
Y(\Theta) \quad &= \quad \left[- \vdash \Theta\right] \\
V(\Theta_i) \quad &= \quad \lim_{i \to \infty} \Theta_i \\
\mathcal{G} \text{ guards } \Theta \quad &\iff \quad \forall \Xi.\ \left[\Xi \vdash \Theta\right] = \sum_{\Gamma \in \mathcal{G}} \left[\Xi \vdash \Gamma\right]\left[\Xi\Gamma \vdash \Theta\right]
\end{aligned}
$$

Way below IND-CCA

$$
\begin{array}{rcl}
 & & [c_0] \\
\cdot[c_0, m = \mathsf{D}(\overline{k}, c_0) & \vdash & m_0, m_1] \\
\cdot[c_0, m = \mathsf{D}(\overline{k}, c_0), m_0, m_1, c \in \mathsf{E}(k, m_b) & \vdash & c_1 \neq c] \\
\cdot[c_0, m = \mathsf{D}(\overline{k}, c_0), m_0, m_1, c \in \mathsf{E}(k, m_b), & & \\
c_1 \neq c, \widetilde{m} = \mathsf{D}(\overline{k}, c_1) & \vdash & b] \quad \leq \quad [b]
\end{array}
$$

Outline

Summary

- an algebraic theory of guessing can be presented as an algebraic theory of approximation
- a probabilistic theory of guessing can be presented by extending $\{0, 1\}$-domains to $[0, 1]$-domains