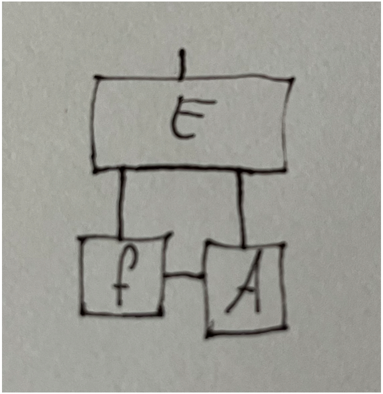
Universal composability is a graded Kleisli category

Andre Knispel

IOG

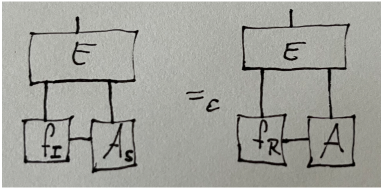
March 19, 2024

The UC experiment



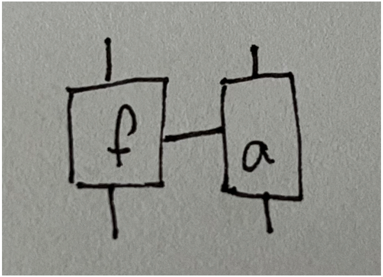
UC-emulation

f_R UC-emulates f_I, if for all A there exists an A_S such that for all E, the following experiments are ε-indistinguishable.



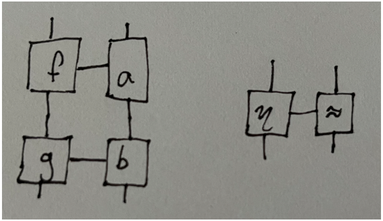
Open adversarial protocols

An open adversarial protocol from (A, C) to (B, D) is a triple (X, f, a) where $f : A \to B \otimes X$ and $a : X \otimes C \to D$. Two OAPs are equivalent if they arise from sliding a morphism $X \to X'$ along the middle wire.



The category of OAPs

Composition of open adversarial protocols is shown on the left (using the monad structure to combine the horizontal wires into one) and the identities are shown on the right, consisting of structure isomorphisms of the monoidal category.



This means that the category of OAPs is the Kleisli category for the graded monad given by the tensor product.

The graded Kleisli construction

Let $\mathcal{M}$ be a $\mathcal{V}$-graded monad on $\mathcal{C}$, i.e. a lax monoidal functor $\mathcal{V} \to End(\mathcal{C})$.

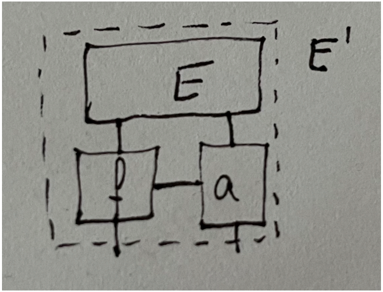
- The objects of $Kl_{\mathcal{M}}$ are pairs of objects of $\mathcal{C}$ and $\mathcal{V}$. Morphisms $(c, x) \to (d, y)$ are triples (z, f, g) where $f : c \to \mathcal{M}_x d$ and $g : z \otimes x \to y$ and equivalence of morphisms is as before.
- The composition and identity structure and laws are given by the monoidal and monad structures.

For notational convenience I'll be omitting z in morphisms from now on.

Environments

The main requirement of an environment is that an environment composed with an OAP is again an environment. If we have a set of environments $\mathcal{E}(S)$ for each object/interface S, given a morphism $(f, a) : S \to T$, there should be a pullback $(f, a)^{-1} : \mathcal{E}(T) \to \mathcal{E}(S)$.

- This means that $\mathcal{E}$ is a presheaf, i.e. a functor $Kl\otimes \to \mathbf{Set}^{op}$.

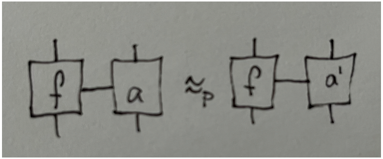


Observational equivalence

- Two OAPs $f, g : S \to T$ are $\mathcal{E}$-observationally equivalent (denoted $f \approx_{\mathcal{E}} g$) if they cannot be distinguished by environments.
- More precisely, $f \approx_{\mathcal{E}} g$ if for all environments $E \in \mathcal{E}(T)$, $f^{-1}E = g^{-1}E$.

Protocol equivalence

Protocol equivalence is the equivalence relation generated by the following:



UC-emulation revisited

Given two OAPs $f, g : S \to T$, f UC-emulates g (denoted $f \leq_{UC} g$) if for all $f' \approx_p f$ there exists a $g' \approx_p g$ such that $f' \approx_{\mathcal{E}} g'$.

Theorem

- Universal composition theorem: $\leq_{UC}$ is preserved by composition.
- Completeness of the dummy adversary: Given two OAPs $(f, id), g : S \to T$, if there exists a $g' \approx_p g$ such that $(f, id) \approx_{\mathcal{E}} g'$ then $f \leq_{UC} g$.

A model: typed, functional UC

Fix a set of *identities*.

- Objects in $\mathbf{UC}_t$ are families of types indexed by identities.
- Morphisms are stateful functions that accept an input on one of the domain or codomain types and may or may not respond on one of the domain or codomain types while updating the state.

Relation to resource theories

- The monoidal structure of $\mathcal{C}$ is preserved into the graded Kleisli construction $Kl\otimes$, so we can apply the Grothendieck construction on the functor of elements.
- $\approx_{\mathcal{E}}$ induces an attack model by $\mathcal{A}_{\mathcal{E}}(f) = \{f' : f \approx_{\mathcal{E}} f'\}$.
- A morphism is $\mathcal{A}_{\mathcal{E}}$-secure iff the morphism corresponding to the adversary is an isomorphism.