2021 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

Quantitative Contract-Based Synthesis and Verification for CPS Security (Award #1739816), August 2017, Alberto Sangiovanni-Vincentelli and Sanjit Seshia, UC Berkeley

Challenge:

- CPSs can undergo modifications during runtime, limiting our ability to ensure their security
- Assume-guarantee (AG) reasoning is used to design and analyze systems compositionally, but existing AG contracts cannot express important security attributes

Solution:

- Completed the development of the algebra of AG contracts
- First results on the theory of hypercontracts, which enables compositional reasoning about arbitrary hyperproperties of CPSs, including non-interference and information-flow constraints, important security requirements

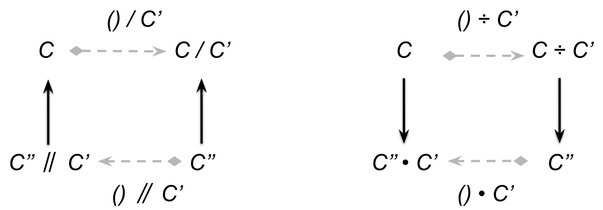
Algebra of Assume-guarantee contracts

Composition
$C_1 \,//\, C_2 = ((A_1 \cap A_2) \cup \neg(G_1 \cap G_2),\ G_1 \cap G_2)$

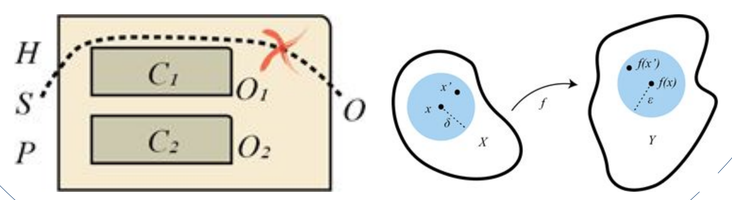
Merging
$C_1 \bullet C_2 = (A_1 \cap A_2,\ (G_1 \cap G_2) \cup \neg(A_1 \cap A_2))$

Quotient
$C / C' = (A \cap G',\ (G \cap A') \cup \neg(A \cap G'))$

Separation
$C \div C' = ((A \cap G') \cup \neg(G \cap A'),\ G \cap A')$



Hypercontracts



Scientific Impact:

- Any research area interested in compositional analysis and design can benefit from our theory

Broader Impact:

- Our work
  - Supports "plug-and-play" methodologies
  - Formalizes component specifications and aids the interaction of an OEM with its suppliers
  - Yields faster design of safer and more secure CPSs
- Our theory is taught in CPS design courses at UC Berkeley