New foundations for probabilistic separation logic

John Li
li.john@northeastern.edu

Amal Ahmed
amal@ccs.neu.edu

Steven Holtzen
s.holtzen@northeastern.edu

Northeastern University
Khoury College of
Computer Sciences

https://john-ml.github.io/lilac.pdf

How to modularly verify probabilistic programs?

How to modularly verify probabilistic programs?

- Probabilistic programs are getting big

How to modularly verify probabilistic programs?

- Probabilistic programs are getting big
- How to perform verification and inference at scale?

How to modularly verify probabilistic programs?

- Idea: break big programs into smaller ones

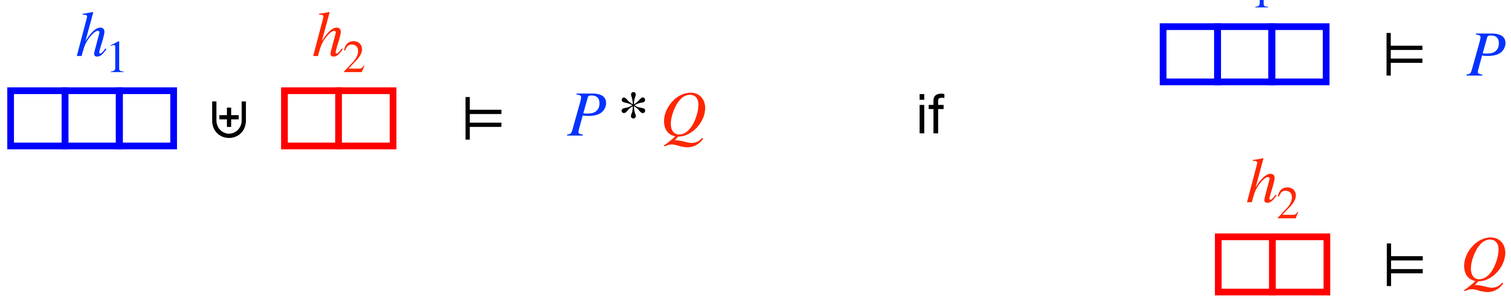
How to modularly verify probabilistic programs?

- Idea: break big programs into smaller ones
- Traditional method: separation logic for modular verification[1]

[1] C. Calcagno and D. Distefano. Infer: An automatic program verifier for memory safety of C programs. NFM 2011.

How to modularly verify probabilistic programs?

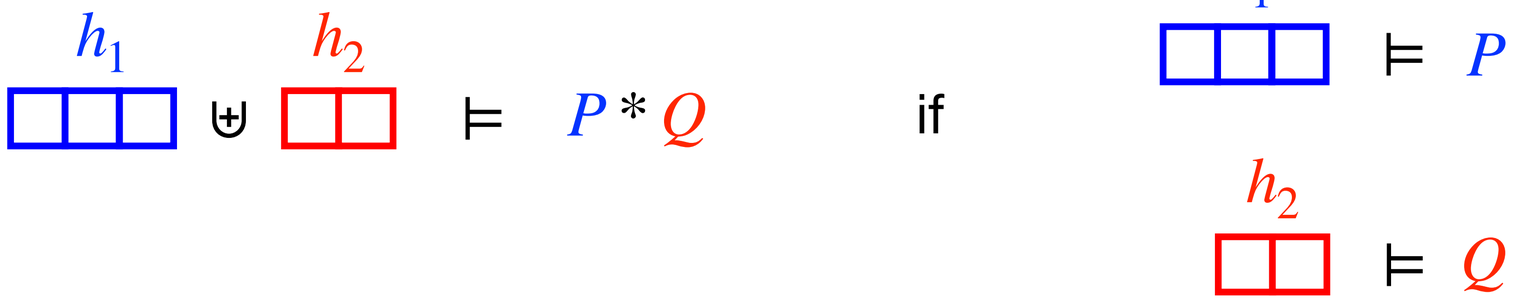
- Idea: break big programs into smaller ones
- Traditional method: separation logic for modular verification[1]



[1] C. Calcagno and D. Distefano. Infer: An automatic program verifier for memory safety of C programs. NFM 2011.

How to modularly verify probabilistic programs?

- Idea: break big programs into smaller ones
- Traditional method: separation logic for modular verification[1]



- Can we adapt this to probabilistic setting?

[1] C. Calcagno and D. Distefano. Infer: An automatic program verifier for memory safety of C programs. NFM 2011.

Traditional heap-separation is not enough

Traditional heap-separation is not enough

A Separation Logic for Concurrent Randomized Programs

JOSEPH TASSAROTTI, Carnegie Mellon University, USA
ROBERT HARPER, Carnegie Mellon University, USA

POPL'19

Quantitative Separation Logic

A Logic for Reasoning about Probabilistic Pointer Programs

KEVIN BATZ, RWTH Aachen University, Germany
BENJAMIN LUCIEN KAMINSKI, RWTH Aachen University, Germany
JOOST-PIETER KATOEN, RWTH Aachen University, Germany
CHRISTOPH MATHEJA, RWTH Aachen University, Germany
THOMAS NOLL, RWTH Aachen University, Germany

POPL'19

Traditional heap-separation is not enough

A Separation Logic for Concurrent Randomized Programs

JOSEPH TASSAROTTI, Carnegie Mellon University, USA
ROBERT HARPER, Carnegie Mellon University, USA

POPL'19

Quantitative Separation Logic

A Logic for Reasoning about Probabilistic Pointer Programs

KEVIN BATZ, RWTH Aachen University, Germany
BENJAMIN LUCIEN KAMINSKI, RWTH Aachen University, Germany
JOOST-PIETER KATOEN, RWTH Aachen University, Germany
CHRISTOPH MATHEJA, RWTH Aachen University, Germany
THOMAS NOLL, RWTH Aachen University, Germany

POPL'19

- With randomness, there's a second resource to account for: probability.

Traditional heap-separation is not enough

A Separation Logic for Concurrent Randomized Programs

JOSEPH TASSAROTTI, Carnegie Mellon University, USA
ROBERT HARPER, Carnegie Mellon University, USA

POPL'19

Quantitative Separation Logic

A Logic for Reasoning about Probabilistic Pointer Programs

KEVIN BATZ, RWTH Aachen University, Germany
BENJAMIN LUCIEN KAMINSKI, RWTH Aachen University, Germany
JOOST-PIETER KATOEN, RWTH Aachen University, Germany
CHRISTOPH MATHEJA, RWTH Aachen University, Germany
THOMAS NOLL, RWTH Aachen University, Germany

POPL'19

- With randomness, there's a second resource to account for: probability.
- Heap-separation doesn't support modular reasoning about this resource.

Separation as statistical independence

Separation as statistical independence

A Probabilistic Separation Logic

GILLES BARTHE, MPI for Security and Privacy, Germany and IMDEA Software Institute, Spain
JUSTIN HSU, University of Wisconsin–Madison, USA
KEVIN LIAO, MPI for Security and Privacy, Germany and University of Illinois Urbana-Champaign, USA

POPL'20

A Separation Logic for Negative Dependence

JIALU BAO, Cornell University, USA
MARCO GABOARDI, Boston University, USA
JUSTIN HSU, Cornell University, USA
JOSEPH TASSAROTTI, Boston College, USA

POPL'22

A Bunched Logic for Conditional Independence

Jialu Bao
University of Wisconsin–Madison

Simon Docherty
University College London

Justin Hsu
University of Wisconsin–Madison

Alexandra Silva
University College London

LICS'21

Separation as statistical independence

A Probabilistic Separation Logic

GILLES BARTHE, MPI for Security and Privacy, Germany and IMDEA Software Institute, Spain
JUSTIN HSU, University of Wisconsin–Madison, USA
KEVIN LIAO, MPI for Security and Privacy, Germany and University of Illinois Urbana-Champaign, USA

POPL'20

A Separation Logic for Negative Dependence

JIALU BAO, Cornell University, USA
MARCO GABOARDI, Boston University, USA
JUSTIN HSU, Cornell University, USA
JOSEPH TASSAROTTI, Boston College, USA

POPL'22

A Bunched Logic for Conditional Independence

Jialu Bao
University of Wisconsin–Madison

Simon Docherty
University College London

Justin Hsu
University of Wisconsin–Madison

Alexandra Silva
University College London

LICS'21

- Propositions modeled by distributions on stores

A new notion of separation

A new notion of separation

- Propositions modeled by *probability spaces*

A new notion of separation

- Propositions modeled by *probability spaces*

A new notion of separation

- Propositions modeled by *probability spaces*

$$\mathscr{P}_1 \bullet \mathscr{P}_2 \models P * Q \quad \text{if} \quad \mathscr{P}_1 \models P \quad \mathscr{P}_2 \models Q$$

A new notion of separation

- Propositions modeled by *probability spaces*

$\mathscr{P}_1 \bullet \mathscr{P}_2 \models P * Q$ if

$\mathscr{P}_1 \models P$

$\mathscr{P}_2 \models Q$

"independent combination"

What does this buy us?

- Standard frame rule
- Continuous variables & equational reasoning
- Conditioning modality $\mathsf{D}_{x \leftarrow X}$
    - Conditional independence: $\mathsf{D}_{x \leftarrow X}(Y * Z)$
    - Other connectives also have intuitive "conditional" readings
- Verified challenging weighted sampling algorithm
- Full paper: https://john-ml.github.io/lilac.pdf