Coupling Proofs Are Probabilistic Product Programs

Gilles Barthe, Benjmain Grégoire, Justin Hsu*, Pierre-Yves Strub

IMDEA Software, Inria, University of Pennsylvania*, École Polytechnique

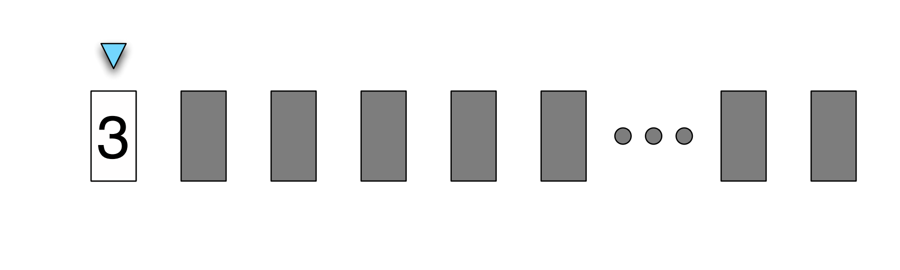
January 18, 2017

A simple card-flipping process

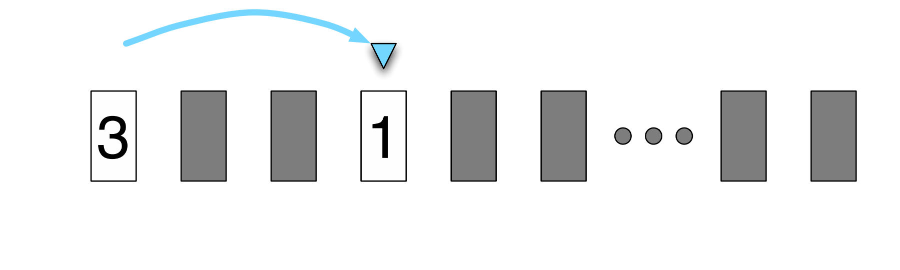
Setup

- Input: position in $\{1, \ldots, 9\}$
- Repeat:
  - Draw uniformly random card $\in \{1, \ldots, 9\}$
  - Go forward that many steps
- Output last position before crossing 100

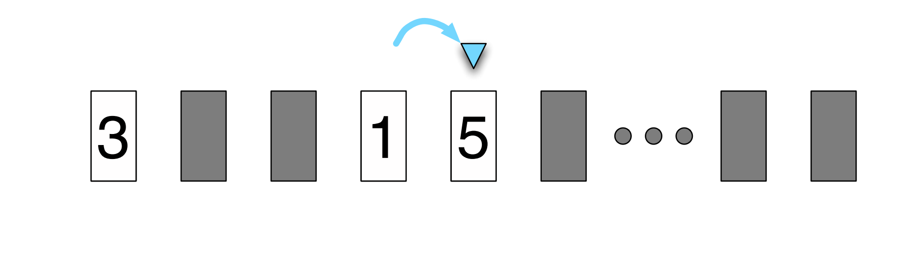
In pictures



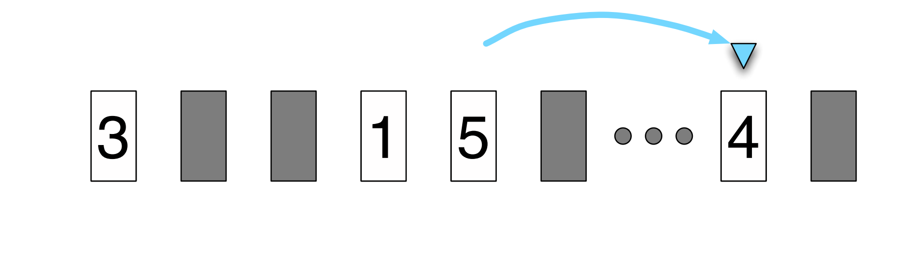
In pictures



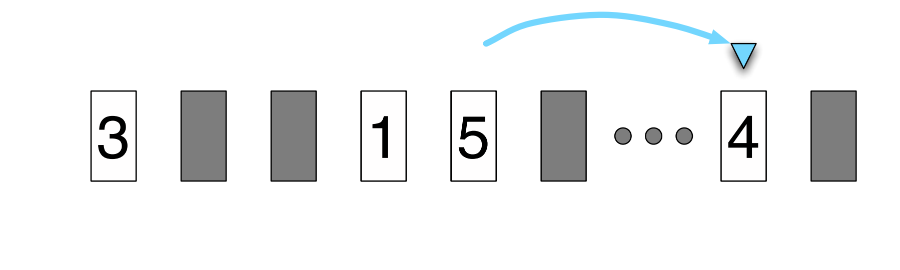
In pictures



In pictures

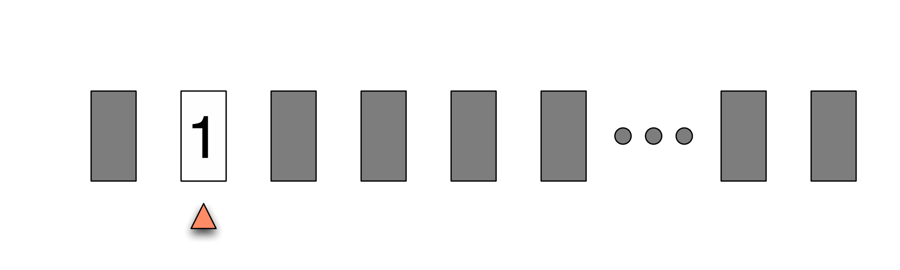


In pictures

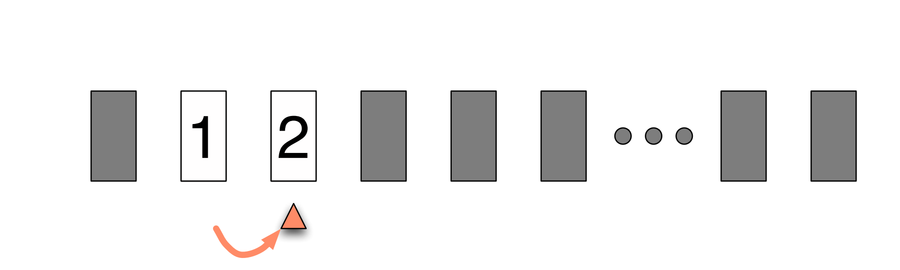


Output last position: 99

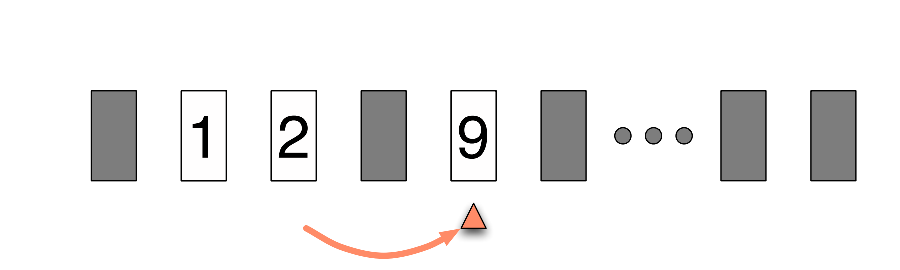
Starting at a different position



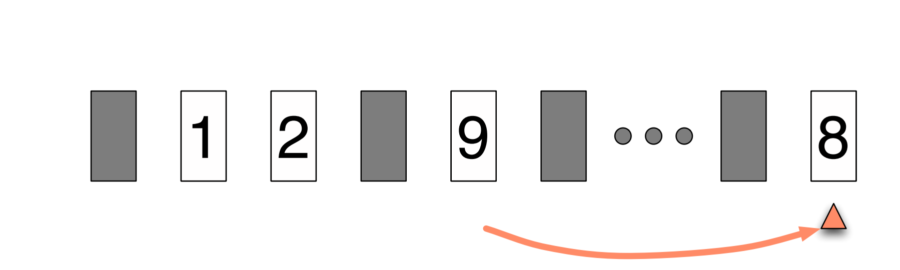
Starting at a different position



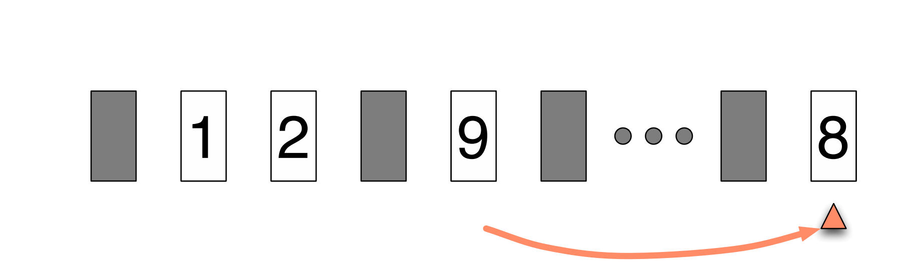
Starting at a different position



Starting at a different position

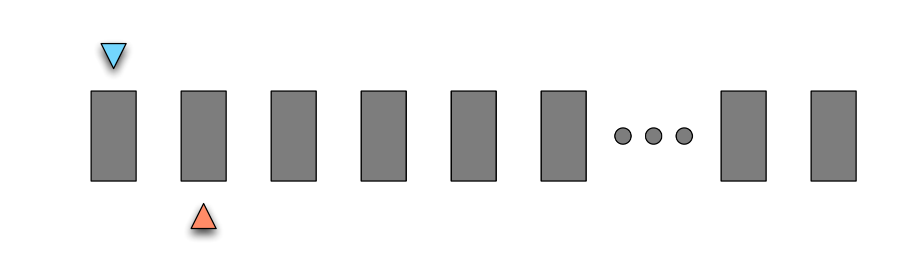


Starting at a different position

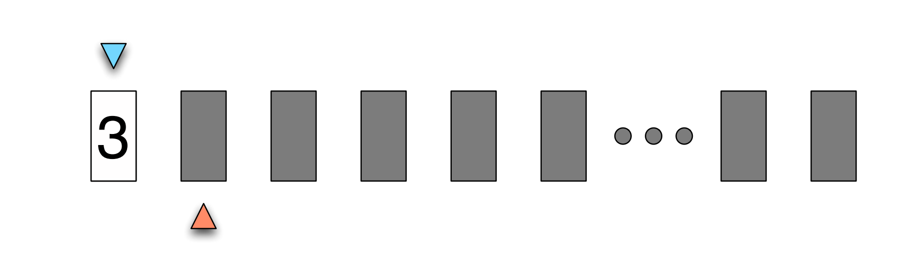


How close are the two output distributions?

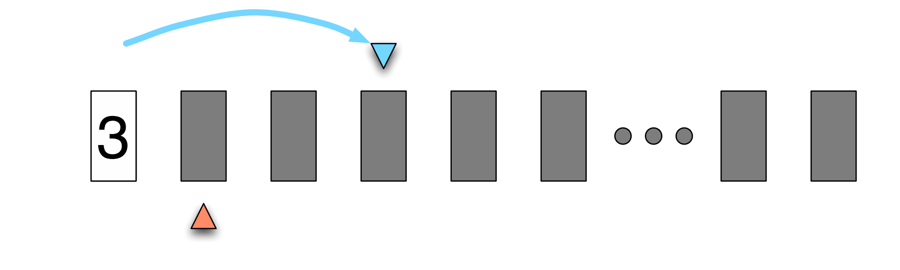
Combine first process and second process



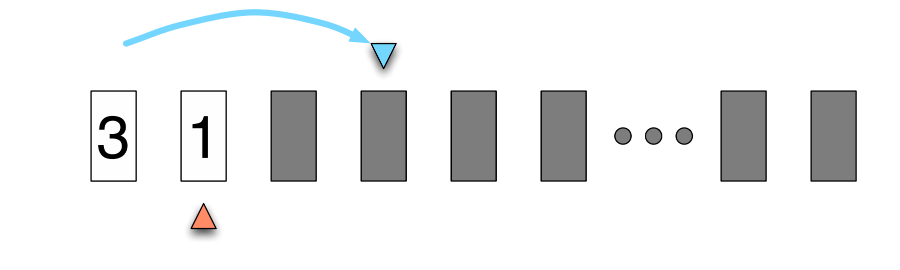
Combine first process and second process



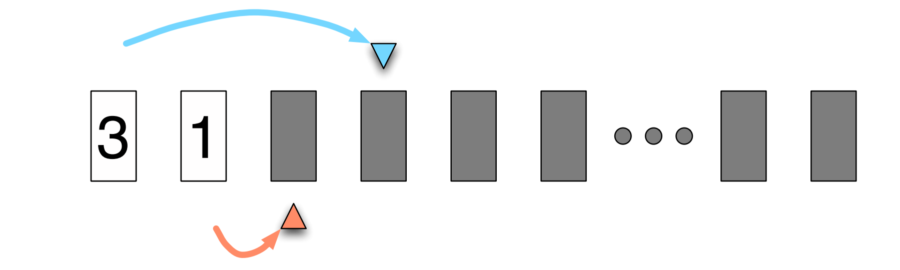
Combine first process and second process



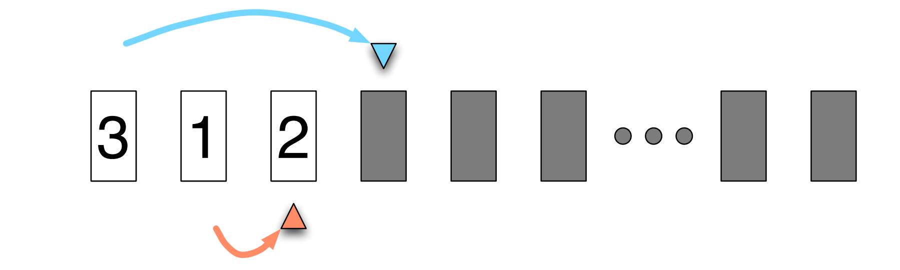
Combine first process and second process



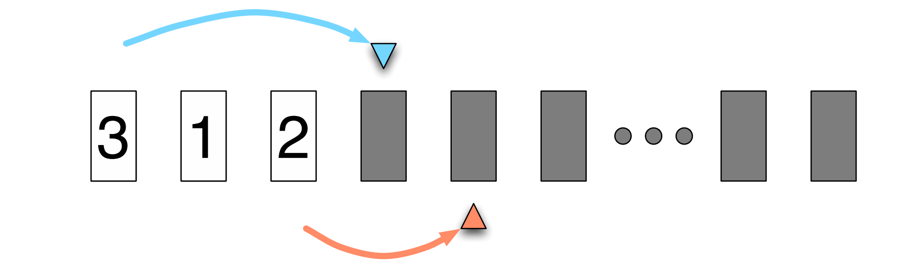
Combine first process and second process



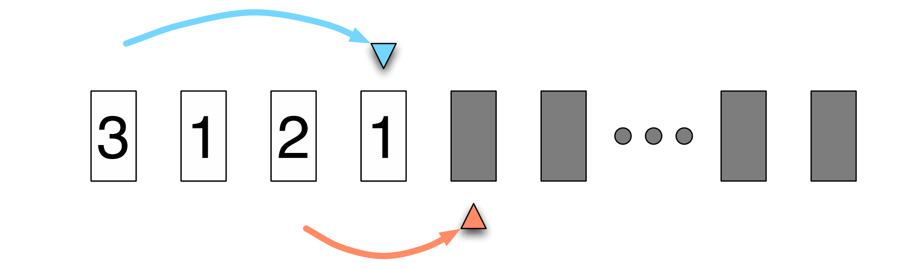
Combine first process and second process



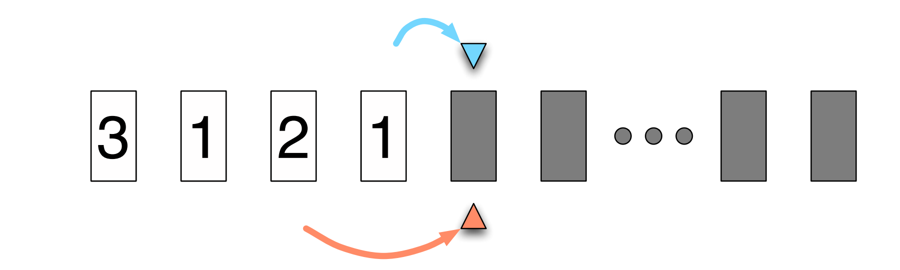
Combine first process and second process



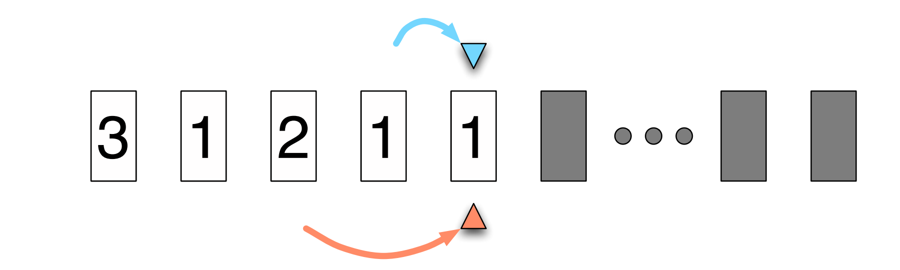
Combine first process and second process



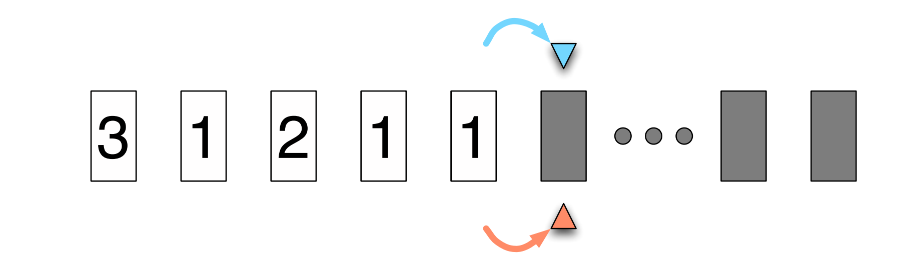
Combine first process and second process



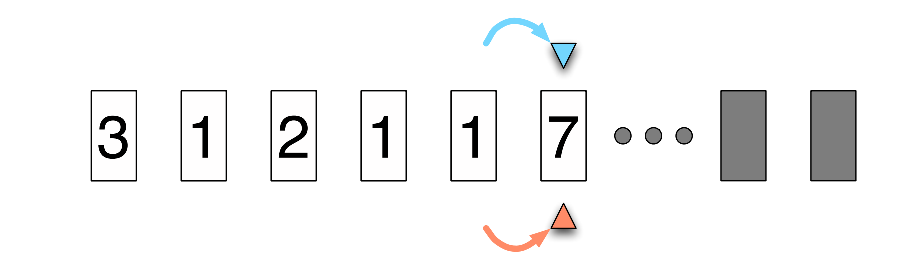
Combine first process and second process



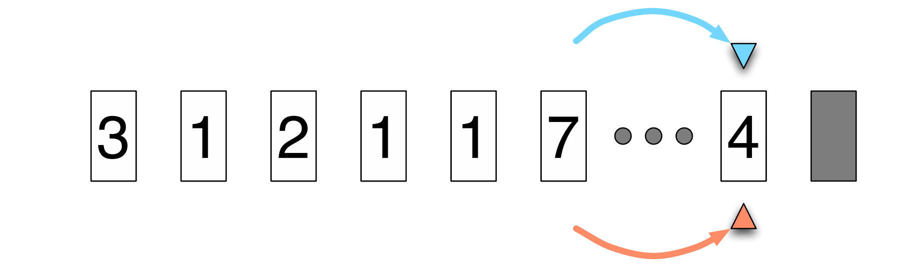
Combine first process and second process



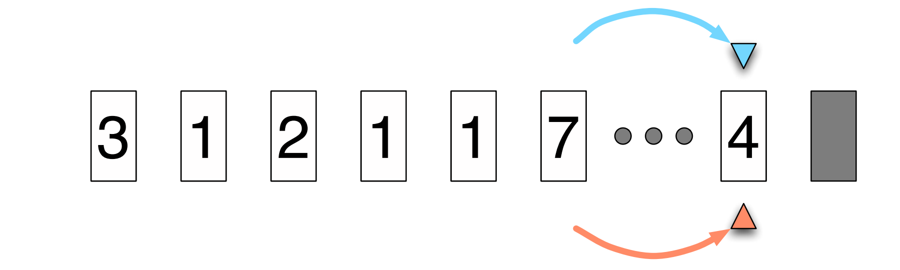
Combine first process and second process



Combine first process and second process



Combine first process and second process



Product program: One program simulating two programs

Why is this interesting?

In general

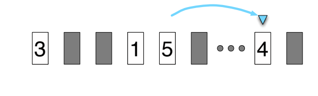
Property P of product program

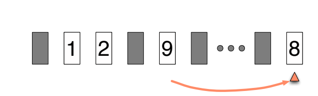
$$\Downarrow$$

Property P' of two programs

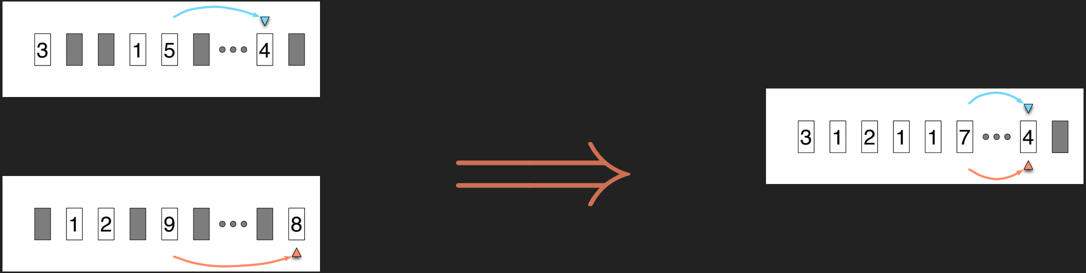
Our construction

Two simulated programs can share randomness

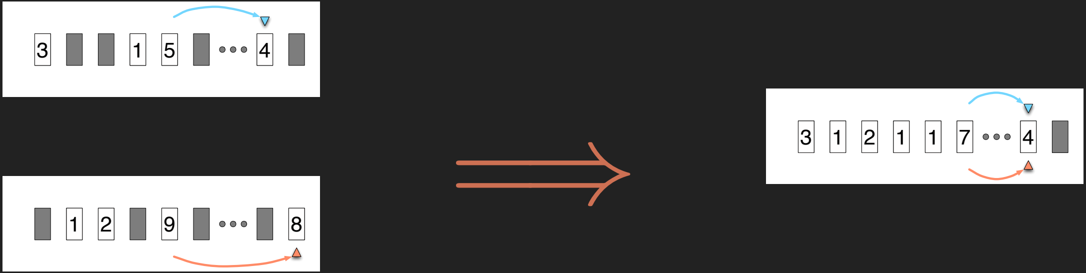




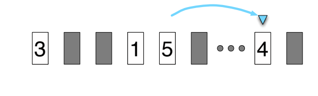
Distance between output distributions

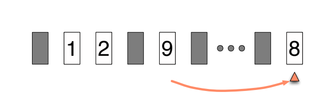


Distance between output distributions

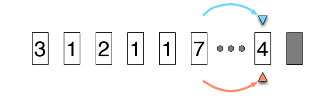


Distance between output distributions $\leq$ Probability that outputs differ





Today:



Distance between output distributions $\leq$ Probability that outputs differ

Our technical contributions

A probabilistic product construction
with shared randomness

A probabilistic program logic $\times$pRHL:
a proof-relevant version of pRHL

A crash course: Probabilistic Relational Hoare Logic [BGZ-B]

Imperative language

$$c ::= x \leftarrow e \mid c \,;\, c \mid \textsf{if } e \textsf{ then } c \textsf{ else } c \mid \textsf{while } e \textsf{ do } c$$

Imperative language

$$c ::= x \leftarrow e \mid c \,;\, c \mid \text{if } e \text{ then } c \text{ else } c \mid \text{while } e \text{ do } c \mid x \xleftarrow{\$} [S]$$

Uniform sampling from finite set $[S]$

- coin flip: [heads, tails]
- random card: [1, . . . , 9]

Imperative language

$$c ::= x \leftarrow e \mid c \,;\, c \mid \text{if } e \text{ then } c \text{ else } c \mid \text{while } e \text{ do } c \mid x \xleftarrow{\$} [S]$$

Uniform sampling from finite set $[S]$

- coin flip: [heads, tails]
- random card: [1, . . . , 9]

Command semantics $[\![c]\!]$

- Input: memory
- Output: distribution over memories

Judgments: similar to Hoare logic

$$\{P\}\ c\ \{Q\}$$

Judgments: similar to Hoare logic

$$\{P\}\ c\ \{Q\}$$

Assertions: binary relation on memories

- Can refer to tagged program variables: $x\langle 1\rangle$ and $x\langle 2\rangle$
- First order formulas, non-probabilistic

Judgments: similar to Hoare logic

$$\{P\}\ c\ \{Q\}$$

Assertions: binary relation on memories

- Can refer to tagged program variables: $x\langle 1\rangle$ and $x\langle 2\rangle$
- First order formulas, non-probabilistic

> If the two inputs satisfy P, we can share the randomness on two runs of c so that the two outputs satisfy Q.

Proof rules in pRHL: mostly similar to Hoare logic

$$\textsc{Assn}\ \frac{}{\{Q\,\{e\langle 1\rangle, e\langle 2\rangle / x\langle 1\rangle, x\langle 2\rangle\}\}\ x \leftarrow e\ \{Q\}} \qquad \textsc{Rand}\ \frac{f : S \to S \text{ bijection}}{\{\forall v \in S, Q\,\{x_1\langle 1\rangle, x_2\langle 2\rangle / v, f(v)\}\}\ x \xleftarrow{\$} [S]\ \{Q\}}$$

$$\textsc{Seq}\ \frac{\{P\}\ c\ \{Q\} \qquad \{Q\}\ c'\ \{R\}}{\{P\}\ c\,;c'\ \{R\}} \qquad \textsc{Cond}\ \frac{\models P \implies e\langle 1\rangle = e\langle 2\rangle \qquad \{P \wedge e\langle 1\rangle\}\ c\ \{Q\} \qquad \{P \wedge \neg e\langle 1\rangle\}\ c'\ \{Q\}}{\{P\}\ \mathsf{if}\ e\ \mathsf{then}\ c\ \mathsf{else}\ c'\ \{Q\}} \qquad \textsc{Loop}\ \frac{\{P \wedge e\langle 1\rangle \wedge e\langle 2\rangle\}\ c\ \{P \wedge e\langle 1\rangle = e\langle 2\rangle\}}{\{P \wedge e\langle 1\rangle = e\langle 2\rangle\}\ \mathsf{while}\ e\ \mathsf{do}\ c\ \{P \wedge \neg e\langle 1\rangle \wedge \neg e\langle 2\rangle\}}$$

$$\textsc{Conseq}\ \frac{\{P\}\ c\ \{Q\} \qquad \models P' \implies P \wedge Q \implies Q'}{\{P'\}\ c\ \{Q'\}} \qquad \textsc{Case}\ \frac{\{P \wedge R\}\ c\ \{Q\} \qquad \{P \wedge \neg R\}\ c\ \{Q\}}{\{P\}\ c\ \{Q\}}$$

Proof rules in pRHL: mostly similar to Hoare logic

$$\textsc{Assn}\ \frac{}{\{Q\,\{e\langle 1\rangle, e\langle 2\rangle / x\langle 1\rangle, x\langle 2\rangle\}\}\ x \leftarrow e\ \{Q\}}$$

$$\textsc{Rand}\ \frac{f : S \to S \text{ bijection}}{\{\forall v \in S, Q\,\{x_1\langle 1\rangle, x_2\langle 2\rangle / v, f(v)\}\}\ x \xleftarrow{\$} [S]\ \{Q\}}$$

$$\textsc{Seq}\ \frac{\{P\}\ c\ \{Q\} \qquad \{Q\}\ c'\ \{R\}}{\{P\}\ c\,;c'\ \{R\}}$$

$$\textsc{Cond}\ \frac{\models P \implies e\langle 1\rangle = e\langle 2\rangle \qquad \{P \land e\langle 1\rangle\}\ c\ \{Q\} \qquad \{P \land \neg e\langle 1\rangle\}\ c'\ \{Q\}}{\{P\}\ \mathsf{if}\ e\ \mathsf{then}\ c\ \mathsf{else}\ c'\ \{Q\}}$$

$$\textsc{Loop}\ \frac{\{P \land e\langle 1\rangle \land e\langle 2\rangle\}\ c\ \{P \land e\langle 1\rangle = e\langle 2\rangle\}}{\{P \land e\langle 1\rangle = e\langle 2\rangle\}\ \mathsf{while}\ e\ \mathsf{do}\ c\ \{P \land \neg e\langle 1\rangle \land \neg e\langle 2\rangle\}}$$

$$\textsc{Conseq}\ \frac{\{P\}\ c\ \{Q\} \qquad \models P' \implies P \land Q \implies Q'}{\{P'\}\ c\ \{Q'\}}$$

$$\textsc{Case}\ \frac{\{P \land R\}\ c\ \{Q\} \qquad \{P \land \neg R\}\ c\ \{Q\}}{\{P\}\ c\ \{Q\}}$$

Proof rules in pRHL: Random sampling

$$\frac{f : S \to S \text{ bijection}}{\{\top\}\; x \xleftarrow{\$} [S]\; \{x\langle 2\rangle = f(x\langle 1\rangle)\}}$$

Proof rules in pRHL: Random sampling

$$\frac{f : S \to S \text{ bijection}}{\{\top\}\ x \xleftarrow{\$} [S]\ \{x\langle 2\rangle = f(x\langle 1\rangle)\}}$$

Select how to share randomness

Introducing ×pRHL

Product pRHL

Idea: Product program $c^{\times}$ simulates two processes

$$\{P\}\ c\ \{Q\}$$

Idea: Product program $c^\times$ simulates two processes

$$\{P\}\ c\ \{Q\} \leadsto c^\times$$

Idea: Product program $c^{\times}$ simulates two processes

$$\{P\}\ c\ \{Q\} \rightsquigarrow c^{\times}$$

Runs in combined memory

- Two separate copies of single memory
- Duplicate program variables: $x\langle 1\rangle$ and $x\langle 2\rangle$

Idea: Product program $c^{\times}$ simulates two processes

$$\{P\}\ c\ \{Q\} \rightsquigarrow c^{\times}$$

Runs in combined memory

- Two separate copies of single memory
- Duplicate program variables: $x\langle 1\rangle$ and $x\langle 2\rangle$

Property of $c^{\times}$ $\implies$ property of two runs of c

A tour of $\times$pRHL rules: [Seq]

In pRHL:

$$\frac{\{P\}\ c\ \{Q\} \qquad \{Q\}\ c'\ \{R\}}{\{P\}\ c\ ;\ c'\ \{R\}}$$

A tour of $\times$pRHL rules: [Seq]

In $\times$pRHL:

$$\frac{\{P\}\; c\; \{Q\} \rightsquigarrow c^{\times} \qquad \{Q\}\; c'\; \{R\} \rightsquigarrow c^{\times\prime}}{\{P\}\; c\,;\, c'\; \{R\} \rightsquigarrow c^{\times}\,;\, c^{\times\prime}}$$

A tour of $\times$pRHL rules: [Seq]

In $\times$pRHL:

$$\frac{\{P\}\ c\ \{Q\} \rightsquigarrow c^{\times} \qquad \{Q\}\ c'\ \{R\} \rightsquigarrow c^{\times\prime}}{\{P\}\ c\ ;\ c'\ \{R\} \rightsquigarrow c^{\times}\ ;\ c^{\times\prime}}$$

Sequence product programs

A tour of $\times$pRHL proof rules: [Rand]

In pRHL:

$$\frac{f : S \to S \text{ bijection}}{\{\top\}\ x \xleftarrow{\$} [S]\ \{x\langle 2\rangle = f(x\langle 1\rangle)\}}$$

A tour of $\times$pRHL proof rules: [Rand]

In $\times$pRHL:

$$\frac{f : S \to S \text{ bijection}}{\{\top\}\ x \xleftarrow{\$} [S]\ \{x\langle 2\rangle = f(x\langle 1\rangle)\} \rightsquigarrow x\langle 1\rangle \xleftarrow{\$} [S]\ ;\ x\langle 2\rangle \leftarrow f(x\langle 1\rangle)}$$

A tour of $\times$pRHL proof rules: [Rand]

In $\times$pRHL:

$$\frac{f : S \to S \text{ bijection}}{\{\top\}\ x \xleftarrow{\$} [S]\ \{x\langle 2\rangle = f(x\langle 1\rangle)\} \rightsquigarrow x\langle 1\rangle \xleftarrow{\$} [S]\ ;\ x\langle 2\rangle \leftarrow f(x\langle 1\rangle)}$$

Sample $x\langle 2\rangle$ depends on $x\langle 1\rangle$

A tour of $\times$pRHL rules: [Case]

In pRHL:

$$\frac{\{P \wedge Q\}\ c\ \{R\} \qquad \{P \wedge \neg Q\}\ c\ \{R\}}{\{P\}\ c\ \{R\}}$$

A tour of $\times$pRHL rules: [Case]

In $\times$pRHL:

$$\frac{\{P \wedge Q\}\ c\ \{R\} \rightsquigarrow c^{\times} \qquad \{P \wedge \neg Q\}\ c\ \{R\} \rightsquigarrow c^{\times}_{\neg}}{\{P\}\ c\ \{R\} \rightsquigarrow \text{if } Q \text{ then } c^{\times} \text{ else } c^{\times}_{\neg}}$$

A tour of $\times$pRHL rules: [Case]

In $\times$pRHL:

$$\frac{\{P \wedge Q\}\ c\ \{R\} \rightsquigarrow c^{\times} \qquad \{P \wedge \neg Q\}\ c\ \{R\} \rightsquigarrow c^{\times}_{\neg}}{\{P\}\ c\ \{R\} \rightsquigarrow \text{if } Q \text{ then } c^{\times} \text{ else } c^{\times}_{\neg}}$$

Case in proof $\rightsquigarrow$ conditional in product

See the paper for ...

Verifying rapid mixing for Markov chains

- Examples from statistical physics
- A cool card trick

Advanced proof rules

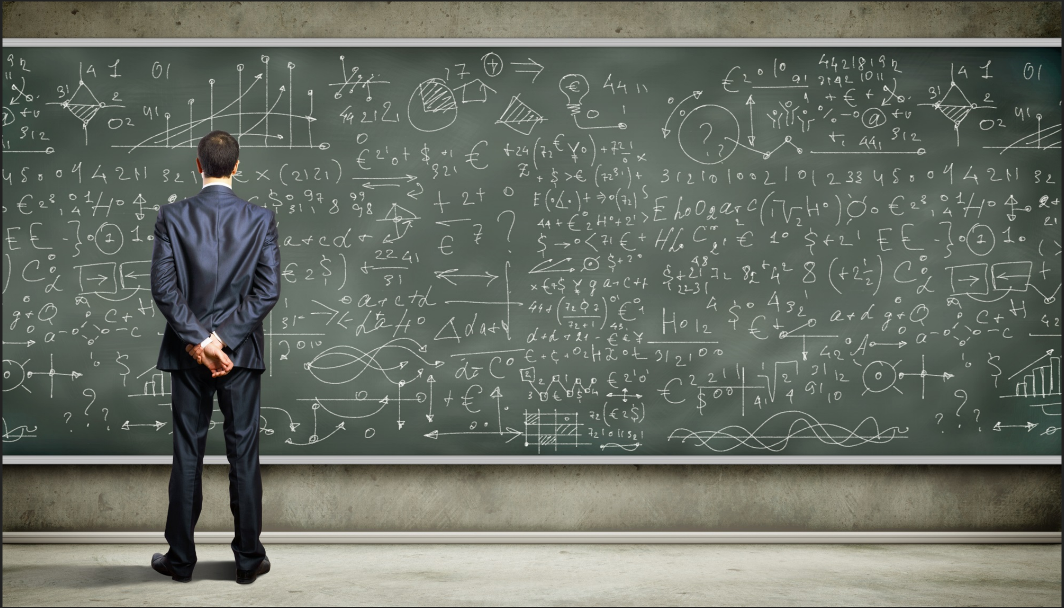
- Asynchronous loop rule

Soundness

Our technical contributions

A probabilistic product construction with shared randomness

A probabilistic program logic $\times$pRHL: a proof-relevant version of pRHL



Proof by coupling

A proof technique from probability theory

- Given: two processes
- Specify: how to coordinate random samplings
- Analyze: properties of linked/coupled processes

Attractive features

- Compositional
- Reason about relation between samples, not probabilities
- Reduce properties of two programs to properties of one program

Coupling proofs $\approx$ pRHL proofs

Coupling proofs $\approx$ pRHL proofs

describe

Two coupled processes

Coupling proofs ≈ pRHL proofs

describe | encode

Two coupled processes ≈ Probabilistic product programs

Coupling proofs ≈ pRHL proofs

describe

encode

Two coupled processes ≈ Probabilistic product programs

Probabilistic product programs are the computational content of coupling proofs