Coupling proofs are probabilistic product programs
Gilles Barthe, Benjamin Grégoire, Justin Hsu, Pierre-Yves Strub

To cite this version:
Gilles Barthe, Benjamin Grégoire, Justin Hsu, Pierre-Yves Strub. Coupling proofs are probabilistic product programs. POPL 2017 - Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, Jan 2017, Paris, France. ACM, 52 (1), pp.161-174, <10.1145/3009837.3009896>. <hal-01649028>

HAL Id: hal-01649028
https://hal.archives-ouvertes.fr/hal-01649028
Submitted on 27 Nov 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Coupling proofs are probabilistic product programs

Gilles Barthe\(^1\)  Benjamin Grégoire\(^2\)  Justin Hsu\(^3\)  Pierre-Yves Strub\(^1\)

IMDEA Software\(^1\)  Inria\(^2\)  University of Pennsylvania\(^3\)

Abstract

Couplings are a powerful mathematical tool for reasoning about pairs of probabilistic processes. Recent developments in formal verification identify a close connection between couplings and pRHL, a relational program logic motivated by applications to provable security, enabling formal construction of couplings from the probability theory literature. However, existing work using pRHL merely shows existence of a coupling and does not give a way to prove quantitative properties about the coupling, which are need to reason about mixing and convergence of probabilistic processes. Furthermore, pRHL is inherently incomplete, and is not able to capture some advanced forms of couplings such as shift couplings. We address both problems as follows.

First, we define an extension of pRHL, called \(\times\) pRHL, which explicitly constructs the coupling in a pRHL derivation in the form of a probabilistic product program that simulates two correlated runs of the original program. Existing verification tools for probabilistic programs can then be directly applied to the probabilistic product to prove quantitative properties of the coupling. Second, we equip \(\times\) pRHL with a new rule for while loops, where reasoning can freely mix synchronized and unsynchronized loop iterations. Our proof rule can capture examples of shift couplings, and the logic is relatively complete for deterministic programs.

We show soundness of \(\times\) pRHL and use it to analyze two classes of examples. First, we verify rapid mixing using different tools from coupling: standard coupling, shift coupling, and path coupling, a compositional principle for combining local couplings into a global coupling. Second, we verify (approximate) equivalence between a source and an optimized program for several instances of loop optimizations from the literature.

1. Introduction

The coupling method \([41, 42, 54, 55]\) is an elegant mathematical tool for analyzing the relationship between probabilistic processes. Informally, couplings correlate outputs of two probabilistic processes by specifying how corresponding sampling statements are correlated; reasoning about the correlated processes can then imply interesting properties of the original processes.

A classical application of couplings is showing that two probabilistic processes converge in distribution. Consider, for instance, a symmetric simple random walk over \(\mathbb{Z}\); starting from some initial position \(p\), the process repeatedly samples a value \(s\) uniformly in \((-1, 1)\) and updates its position to \(p + s\). As the process evolves, the distribution on position spreads out from its initial position, and converges to a limit distribution that is the same for all initial positions. This property can be proved by constructing a coupling where the probability that the two coupled walks end in the same position approaches 1 as we run process.

Beyond merely showing convergence, typically we are interested in how quickly the processes converge. The rate of convergence, sometimes measured by the mixing time of a process, is highly important \([41]\). A common use of probabilistic processes is to efficiently sample from a distribution that approximates a complicated distribution (e.g., Metropolis et al. \([43]\)). For instance, the Glauber dynamics \([33]\) approximately samples from the uniform distribution on proper colorings of a graph—a hard distribution to compute—by maintaining a coloring and randomly re-coloring a single vertex at a time. More generally, the Glauber dynamics is an example of Markov Chain Monte-Carlo (MCMC), a family of techniques that underlie many computational simulations in science, and machine learning algorithms for performing probabilistic inference (see Brooks et al. \([22]\) for a survey). The mixing time determines how many steps we need to run the process before we are approximately sampling from the target distribution.

Recently, Barthe et al. \([12]\) noticed a close connection between couplings and probabilistic relational Hoare logic (pRHL), originally designed for reasoning about the computational security of cryptographic constructions \([5]\). Namely, every valid derivation in pRHL implies the existence of a coupling of the output distributions of the two programs. Using this observation, Barthe et al. \([12]\) verify pRHL judgments that imply properties of random walks, the balls-in-bins process, and the birth-death process. Barthe et al. \([13]\) extend the connection to approximate couplings in approximate probabilistic relational Hoare logic (apRHL), introduced for reasoning about differentially private computations \([7]\), and exploit this connection to prove differential privacy of several examples that had previously been beyond the reach of formal verification.

While pRHL is a useful tool for constructing couplings, it has two limitations. First, it cannot directly reason about the two coupled processes. This poses a problem for proving mixing and convergence properties. For instance, Barthe et al. \([12]\) prove that if a certain property \(P\) holds on the coupled samples, then two random walks meet under the coupling. By a theorem about random walks, this means that the (total variation) distance between the two distributions is at most the probability of \(P\) under the coupling. However, we do not know what this probability is or how it grows as we run the random walk for more iterations, since pRHL cannot reason about the coupled process. We run into similar difficulties if we try to prove convergence using path coupling \([23]\), a general construction that shows fast convergence by upper-bounding the expected distance when we make a transition from two coupled states. While we can express the transition function in code, pRHL cannot reason about expectations.
Second, pRHL cannot express some natural classes of couplings because the rule for \texttt{while} loops requires that both loops execute in lockstep. For instance, \textit{shift couplings} allow the two processes to meet at a random time shift, e.g., the first process at time \(t_1\) could track the second process at some other time \(t_2 = t_1 + \delta\). This incompleteness of pRHL is also a limitation for more standard applications of pRHL to program analysis, like validation of loop transformations, and more generally for any optimization that alters the control flow of the programs.

We address these problems as follows. First, we deepen the connection between pRHL and couplings with an observation that is reminiscent of proofs-as-programs: not only do pRHL judgements correspond to couplings, but pRHL \textit{proofs} encode a \textit{probabilistic product program} that constructs the distribution witnessing the coupling. This program is similar to existing product program constructions \[6, 57\] in that it simulates two program executions with a single program. However, the probabilistic product also coordinates the samplings in the two executions, as specified by the coupling encoded in the original pRHL derivation. Second, we propose a general rule for \texttt{while} loops; our rule subsumes several existing rules and is sufficiently expressive to capture several examples of shift coupling. The resulting system, which we call \textit{product} pRHL or \(\times\text{pRHL}\) for short, has several benefits.

First, we obtain a simple, algorithmic procedure to construct the probabilistic product given a pRHL derivation. The product directly simulates the coupled processes, so we can prove quantitative properties about probabilities or expected values of this coupling using existing probabilistic verification techniques. Moreover, intermediate assertions in a pRHL derivation to be soundly transported to the probabilistic product in \(\times\text{pRHL}\) derivations. For instance, we may prove synchronized control flow in pRHL, and directly assume this fact in the probabilistic product. Many facts are often practically easier to manipulate in pRHL, since pRHL works purely on non-probabilistic assertions.

Second, we obtain a powerful logic that can reason about many examples from the coupling literature, especially shift couplings, and from the translation validation literature, especially loop optimizations. On the foundational side, we prove that our logic is relatively complete for deterministic programs.

\textbf{Summary of contributions} We make the following contributions.

- We present a proof-relevant program logic \(\times\text{pRHL}\) that extracts a probabilistic product program from a valid derivation, and prove (using the Coq proof assistant) that the logic is sound.
- We propose new rules for loops and random sampling in \(\times\text{pRHL}\).
- We also prove relative completeness for deterministic programs.
- We demonstrate several applications of \(\times\text{pRHL}\) to showing convergence of probabilistic processes; several of these examples use path coupling, a compositional tool for constructing couplings which bounds convergence in terms of expected properties of the coupling, and shift coupling, a generalization of coupling where the two processes are allowed to meet at different times. We also show how to validate some common loop transformations.

2. Preliminaries

We begin by giving a bird’s eye view on probabilistic couplings, which take output distributions from two probabilistic processes and place them in the same probabilistic space.

In the following, we will work with sub-distributions over discrete (finite or countable) sets.

\textbf{Definition 1.} A discrete sub-distribution over a set \(A\) is completely defined by its mass function \(\mu : A \rightarrow [0, 1]\) such that \(\sum_{a \in A} \mu(a)\) is defined and bound by 1. The quantity \(\sum_{a \in A} \mu(a) \in [0, 1]\) is called the \textit{weight} of \(\mu\) and denoted by \(|\mu|\). The support \(\text{supp}(\mu)\) of \(\mu\) is defined as \(\{x \in A \mid \mu(x) \neq 0\}\) and is discrete (i.e., countable) by construction. A \textit{distribution} is a sub-distribution with weight 1. The probability of an event \(P\) w.r.t. \(\mu\), written \(\Pr_{\mu}[P]\) (or \(\Pr[P]\) when \(\mu\) is clear from the context), is defined as \(\sum_{x \in P} \mu(x)\).

One can equip distributions with a monadic structure using the Dirac distributions \(1_x\) for the unit and \textit{distribution expectation} \(\mathbb{E}_{x \sim \mu}[M(x)]\) for the bind, where

\[\mathbb{E}_{x \sim \mu}[M(x)] : x \mapsto \sum_{a} \mu(a) \cdot M(a)(x).\]

When working with sub-distributions over tuples, the probabilistic versions of the usual projections on tuples are called \textit{marginals}. For distributions over pairs, we define the first and second marginals \(\pi_1(\mu)\) and \(\pi_2(\mu)\) of a distribution \(\mu\) over \(A \times B\) by \(\pi_1(\mu)(a) = \sum_{b} \mu(a, b)\) and \(\pi_2(\mu)(b) = \sum_{a} \mu(a, b)\). For a distribution \(\mu\) over memories and a set of variables \(X \subseteq \text{Vars}\), we define the \(X\)-\textit{marginal distribution} of \(\mu\) as

\[\pi_X(\mu)(\bar{x}) = \sum_{v \in \text{Vars} \setminus X} \mu(\bar{x}, v).\]

We can also construct a sub-distribution over tuples from two distributions: the \textit{product} sub-distribution of sub-distributions \(\mu_1\) and \(\mu_2\) over \(A\) and \(B\) respectively is defined by

\[(\mu_1 \times \mu_2)(a, b) = \mu_1(a) \cdot \mu_2(b).\]

We are now ready to formally define coupling.

\textbf{Definition 2.} Two sub-distributions \(\mu_1, \mu_2\) resp. over \(A\) and \(B\) are said to be \textit{coupled} with witness \(\mu \in \text{Distr}(A \times B)\), written \(\mu \bullet (\mu_1 \& \mu_2)\), if \(\pi_1(\mu) = \mu_1\) and \(\pi_2(\mu) = \mu_2\).

For \(\Psi \subseteq A \times B\), we write \(\mu \bullet_{\Psi} (\mu_1 \& \mu_2)\) if \(\mu \bullet (\mu_1 \& \mu_2)\) and moreover \(\text{supp}(\mu) \subseteq \Psi\). We will often abuse notation and call \(\mu\) a coupling of \(\mu_1\) and \(\mu_2\).

As an example, suppose that \(A = B\) and \(\mu_1 = \mu_2\) are the uniform distributions. Then, any bijection \(f : A \rightarrow A\) gives a coupling of \(\mu_1\) and \(\mu_2\); we call the resulting coupling \(D_f(A)\) so that \(D_f(A) \bullet (\mu_1 \& \mu_2)\). The coupling \(D_f(A)\) assigns positive probability only to pairs \((v, v)\) with \(v \in A\).

For another example, suppose again that \(A = B\) and \(\mu_1 = \mu_2\), but the distributions are not necessarily uniform. Then, the identity map \(\text{id}_A : A \rightarrow A\) always gives a coupling of \(\mu_1\) and \(\mu_2\); correling samples from both distributions to be the same. We will write \(D^\ast(\mu_1)\) for the resulting coupling, so that \(D^\ast(\mu_1) \bullet (\mu_1 \& \mu_2)\). If \(\mu_1\) is the uniform distribution we will sometime write \(D^\ast(A)\) instead of \(D^\ast(\mu_1)\). Note that \(D^\ast(\mu_1)\) assigns positive probability only to pairs \((v, v)\) with \(\mu_1(v), \mu_2(v) \neq 0\).

To reason about convergence of probabilistic processes, we will use the total variation distance on distributions (also known as statistical distance).

\textbf{Definition 3.} Let \(\mu_1\) and \(\mu_2\) be sub-distributions over a countable set \(A\). The \textit{total variation} (TV) distance between \(\mu_1\) and \(\mu_2\) is defined by:

\[\text{TV}(\mu_1, \mu_2) = \frac{1}{2} \sum_{a \in A} |\mu_1(a) - \mu_2(a)|.\]

To bound this distance, it is enough to find a coupling and bound the probability that the two coupled variables differ; this is the fundamental idea underlying the coupling method.

\[1\] is the distribution where \(x\) has probability 1 and all other elements have probability 0.
Theorem 4 (Fundamental theorem of couplings (e.g., [42])). Let $\mu_1$ and $\mu_2$ be distributions over a countable set. Then for any coupling $\mu$ of $\mu_1, \mu_2$, we have

$$TV(\mu_1, \mu_2) \leq Pr(x, x') - \mu[x \neq x'].$$

3. Product programs

3.1 Language

We will work with a core, probabilistic imperative language with a command for random sampling from primitive distributions. The set of commands is defined as follows:

$$C ::= \text{skip} \mid \text{noop} \mid \text{abort} \mid \text{X} \leftarrow \text{E} \mid \text{X} \leftrightarrow \text{D}(\mathcal{E}) \mid \Phi[C; C] \mid \text{if E then C else C} \mid \text{while E do C} \mid \text{while loop}$$

Here, $\mathcal{X}$ is a set of variables, $\mathcal{E}$ is a set of (deterministic) expressions, and $\mathcal{D}$ is a set of distribution expressions. Variables and expressions are typed, ranging over booleans, integers, lists, etc. The expression grammar is entirely standard, and we omit it.

We will use several shorthands for commands: if $e$ then $c$ for if $e$ then $c$ else skip, abort for the looping command while $\top$ do skip, and $e^c,k$ for the $k$-fold composition of $c$ restricted to $e$. Formally,

$$e^c,k \triangleq \begin{cases} 0, & \text{if } k = 0; \\ (i < k) \land e \text{ do } c; i++; & \text{for any fresh variable } i, \text{ when } k \text{ is a constant,} \end{cases}$$

for the simple notion of program equivalence introduced in Figure 2.

The denotational semantics of programs is adapted from the seminal work of Kozen [30]. We first interpret every ground type $T$ as a set $[T]$; other constructors $C$ are interpreted as functions $[C]$ that respect their arities. The semantics of expressions and distribution expressions is then parameterized by a state $m$, and is defined in the usual way. Last, commands are interpreted as a function from memories to sub-distributions over memories, where memories are finite maps, so $\text{State}_X$ denotes the set of memories over the finite set of variables $X$. Moreover, we use $\upsilon$ to denote the standard disjoint union on finite maps, so $\upsilon : \text{State}_X \times \text{State}_X \to \text{State}_{X \cup X}$ for disjoint finite sets $X_1$ and $X_2$. The interpretation of $c$, written $[c]$, is a function from $\text{State}_X$ to $\text{Distr}(\text{State}_X)$, where $\text{Vars}(c) = X$.

The definition of $[\cdot]$ is given in Figure 1.

3.2 Proof system

Our proof system manipulates judgments of the form:

$$\{ \Phi \} \begin{array}{c} c_1 \\ c_2 \end{array} \{ \Psi \} \rightsquigarrow c$$

where $c_1, c_2$ and $c$ are statements over disjoint variables, and $\Phi$ and $\Psi$ are assertions over the variables of $c_1$ and $c_2$. We will not fix a specific syntax for assertions, but one natural choice is first-order formulas over the program variables of both programs.

Informally, the judgment is valid if $c$ is a probabilistic product program for $c_1$ and $c_2$ under the pre-condition $\Phi$, i.e. for every initial memory $m = m_1 \uplus m_2$ satisfying the pre-condition $\Phi$, the sub-distribution $[c]_m$ is a coupling for $[c_1]_{m_1}$ and $[c_2]_{m_2}$, and moreover $\text{supp}([c]_m)$ only contains states that satisfy $\Psi$.

Definition 5 (Valid judgment).

- Two commands $c_1$ and $c_2$ are separable iff their variables are disjoint, i.e. $\text{Vars}(c_1) \cap \text{Vars}(c_2) = \emptyset$.
- A judgment $\{ \Phi \} \begin{array}{c} c_1 \\ c_2 \end{array} \{ \Psi \} \rightsquigarrow c$ is valid iff the commands $c_1$ and $c_2$ are separable and for every memory $m = m_1 \uplus m_2$ such that $m \vdash \Phi$, we have $[c]_m \triangleleft \Phi \langle ([c_1]_{m_1}) \bowtie ([c_2]_{m_2}) \rangle$.

For comparison, judgments in pRHL are of the form

$$\{ \Phi \} c_1 \begin{array}{c} c_2 \end{array} \{ \Psi \}$$

and assert that for every initial memory $m = m_1 \uplus m_2$ such that $m \vdash \Phi$, there exists a coupling $\mu$ such that

$$\mu \triangleleft \Phi \langle ([c_1]_{m_1}) \bowtie ([c_2]_{m_2}) \rangle.$$

In contrast, our notion of judgment is proof-relevant, since the derivation of the judgment guides the product construction. We briefly comment on several rules in our system, presented in Fig. 3.

The [CONSEQ] rule is similar to the rule of consequence, and reflects that validity is preserved by weakening the post-condition and strengthening the pre-condition; none of the programs is modified in this case.

The [FALSE] rule corresponds to the fact that under a false precondition nothing needs to be proved.

The [CASE] rule allows proving a judgment by case analysis; specifically, the validity of a judgment with pre-condition $\Phi$ can be established from the validity of two judgments, one where the pre-condition is strengthened with $c$ and the other where the pre-condition is strengthened with $\neg c$. The product program is of the form $e$ if $e$ then $c$ else $c'$, where $c$ and $c'$ correspond to the product programs built from the proofs of the first and second premises respectively.

The [STRUCT] rule allows replacing programs by provably equivalent programs. The rules for proving program equivalence are given in Figure 2 and manipulate judgments of the form $\Phi \vdash e \equiv c'$, where $\Phi$ is a relational assertion. We only introduce equations that are needed for recovering derived rules, striving to keep the notion of structural equivalence as simple as possible.

The [ASSG] rule corresponds to the pRHL rule for assignments; in this case, the product program is simply the sequential composition of the two assignments.

The [RAND] rule informally takes a coupling between the two distributions used for sampling in the left and right program, and produces a product program that draws the pair of correlated samples from the coupling. Since our language supports sampling from distribution expressions and not only distributions, the rule asks for the existence of a coupling for each interpretation of the distribution expressions under a valuation satisfying the pre-condition $\Phi$ of the judgment. Furthermore, note that the rule requires that every element in the support of the coupling validates the post-condition. This is similar to pRHL, and is a natural requirement given the notion of valid judgment. However, the rule is strictly more general than the corresponding pRHL rule, which is restricted to the case where $\Psi$ is the graph of some bijection.

The [WHILE] rule for while loops constructs a product program that interleaves synchronous and asynchronous executions of the loop bodies. The first premise establishes that $k_1$ and $k_2$ are strictly
positive when the loop invariant $\Psi$ holds. Then, we specify an expression $c$—which may mention variables from both sides—that holds true exactly when at least one of the guards is true.

Next, the notation $\oplus \{(p_0, p_1, p_2)\}$ indicates that exactly one of the tests $p_0$, $p_1$, and $p_2$ must hold. These predicates guide the construction of the product program. If $p_0$ holds, then both guards should be equal and we can execute the two sides $k_1$ and $k_2$ iterations respectively, preserving the loop invariant $\Psi$. If $p_1$ holds and the right loop has not terminated yet, then the left loop also has not terminated yet and we may execute the left loop one iteration. If $p_2$ holds and the left loop has not terminated yet, then the right loop also has not terminated yet and we may execute the right loop one iteration.

The last pair of premises deal with termination. Note that some condition on termination is needed for soundness of the logic; if the left loop terminates with probability 1 while the right loop terminates with probability 0 (i.e., never), it is impossible to construct a valid product program since there is no distribution on pairs that has first marginal with weight 1 and second marginal with weight 0. So, we require that the first and second loops are lossless assuming $p_1$ and $p_2$ respectively. This ensures that with probability 1, there are only finitely many steps where we execute the left or right loop separately. Note that the product program may still fail to terminate with positive probability since there may be infinite sequences of iterations where $p_0$ holds so both loops advance, but both programs will yield sub-distributions with the same weight so we can still find a coupling.

With these premises, the construction of the product program is straightforward. At the top level, the product continues as long as $e$ is true, i.e., while at least one of the two loops can make progress. Each iteration, it performs a case analysis on the three predicates. If $p_0$ holds, then we execute the product from running the two loops $k_1$ and $k_2$ iterations respectively. If $p_1$ holds, then we execute the product from running the left loop one iteration; if $p_2$ holds then we execute the product from running the right loop one iteration.

**Derived rules**

Presentations of relational Hoare logic often include one-sided rules, which are based on the analysis of a single program (rather than two). By reasoning about program equivalence, we can derive all one-sided rules and the two-sided rules of conditionals and loops from pRL, presented in Fig. 1 within our system.²

**Proposition 6. All the rules in Figure 1 (and their symmetric version) are derived rules.**

We briefly comment on some of the derived rules. The [ASSG-L] rule is the one-sided rule for assignment. It can be derived from its two-sided counterpart, the [ASSG] rule, using the [STRUCT] rule.

² In fact, the one-sided and two-sided rules are inter-derivable for all constructions except random assignments and loops.

---

**Figure 1.** Interpretation of commands

<table>
<thead>
<tr>
<th>$\Phi \vdash c \equiv c$</th>
<th>$\Phi \vdash c_1 \equiv c_2$</th>
<th>$\Phi \vdash _x \equiv \text{skip}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Phi \vdash (x_1, x_2) \equiv _1 \times _2 \equiv (x_1, x_2)$</td>
<td>$\top \vdash c_2 \equiv c_1$</td>
<td>$\top \vdash _x \equiv \text{skip}; c \equiv c$</td>
</tr>
<tr>
<td>$\Phi \equiv x \equiv e \equiv c$</td>
<td>$\Phi \vdash c_1 \equiv c'_1 \land c_2 \equiv c'_2$</td>
<td>$\Phi \equiv _e \equiv _e$</td>
</tr>
<tr>
<td>$\Phi \equiv \text{if } e \text{ then } c \equiv \text{if } e \text{ else } c' \equiv c' \equiv c'$</td>
<td>$\Phi \equiv \text{if } e \text{ then } c_1 \equiv \text{if } e \text{ else } c'_1 \equiv c'_2$</td>
<td>$\Phi \equiv \text{while } e \equiv \text{do } c \equiv \text{while } e \equiv \text{do } c'$</td>
</tr>
<tr>
<td>$\Phi \equiv \text{while } e \equiv \text{do } c \equiv \text{if } e \text{ then } (c; \text{while } e \equiv \text{do } c)$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

The [RAND-L] rule is the one-sided rule for random sampling. It can be derived from its two-sided counterpart, the [RAND] rule, using the [STRUCT] rule and the fact that the product distribution $\mu_1 \times \mu_2$ is a valid coupling of proper distributions $\mu_1$ and $\mu_2$.

We have one-sided and two-sided rules for conditionals. The [COND-L] rule is the one-sided version; it can be derived from the [CASE] and [STRUCT] rules. The [COND-S] rule is the two-sided version; the rule assumes that the two guards of the conditional statements are synchronized, so that one must only need to reason about the cases where both statements enter the true branch, and the case where both statements enter the false branch. It can be derived from the [CASE], [STRUCT], and [FALSE] rules.

We also have one-sided and two-sided rules for loops. The [WHILE-L] rule corresponds to the pRL one-sided rule for while loops; it can be derived from the [WHILE] rule by setting $p_1 = \top$, $p_0 = p_2 = \bot$, and $k_1 = k_2 = 1$, $e \equiv c_1$, $c_2 \equiv \bot$, $c_2 = \text{skip}$ and using the [STRUCT] and [FALSE] rules. The rule [WHILE-S] corresponds to the pRL two-sided rule for while loops. This rule assumes that the two loops are synchronized, i.e., the guards of the two loops are equal assuming the loop invariant. This rule can be derived from the general [WHILE] rule by setting $p_0 = \top$, $p_1 = \bot$, $p_2 = 1$, and $k_1 = k_2 = 1$, $e \equiv c_1$, $c_2 \equiv \bot$, $c_2 = \text{skip}$. 
3.3 Soundness and (relative) completeness

We have formally verified the soundness theorem below in the Coq proof assistant, with Sreerat.

**Theorem 7 (Soundness).** Every derivable judgment is valid.

*Proof sketch.* By induction on the proof derivation. The most interesting case is the loop rule, which we briefly sketch here. We will use the same notations from Fig. 3. Proving that the program satisfies the post-condition is immediate by construction, the condition $e$ does not hold after the execution of the loop. Moreover, the premises ensure that the loop body of the product preserves the invariant $\Psi$. So, we just need to prove that the semantics of the projections of the program correspond to the respective semantics of the original programs. We detail the first projection, i.e. that for any initial memory $m$ s.t. $m \models \Psi$, we have

$$\left\lfloor w_1 \right\rfloor_{m} = \pi_1 \left( \left\lfloor w \right\rfloor_{m} \right)$$

(1)

where $w \triangleq \text{while } e \text{ do } c$ and $w_i \triangleq \text{while } e_i \text{ do } c_i$; the other projection is similar. By definition, we have for any $e$ and $c$

$$\left\lfloor e \right\rfloor_{m} = \lim_{n \to \infty} \left\lfloor c_{e,n} \right\rfloor_{m}$$

Since $\left\lfloor c_{e,n} \right\rfloor_{m}$ is monotonic in $n$, proving Eq. (1) amounts to showing

$$\left\lfloor e_1 \right\rfloor_{m} \leq \pi_1 \left( \left\lfloor w \right\rfloor_{m} \right)$$

(2)

$$\pi_1 \left( \left\lfloor c_{e,n} \right\rfloor_{m} \right) \leq \left\lfloor \text{true} \right\rfloor_{m}$$

(3)

for all $n$. We proceed by induction on $n$. Let $m_i \triangleq \pi_i \left( m \right)$ for $i \in \{1, 2\}$. The base case is immediate and we consider the $n+1$ case. We will prove (2) by case analysis on $\left\lfloor e_1 \right\rfloor_{m}$ and $\left\lfloor w \right\rfloor_{m}$. If $\left\lfloor e_1 \right\rfloor_{m}$ does not hold, then $\left\lfloor c_{e_1,n} \right\rfloor_{m_1} = 1_{m_1}$. Now if $\left\lfloor c_{e_2,n} \right\rfloor_{m_1}$ is false, then $\left\lfloor c_{e_2,n} \right\rfloor_{m_1}$ is also false and (2) holds. Otherwise if $\left\lfloor c_{e_2,n} \right\rfloor_{m_1}$ is true, $\left\lfloor p_{0_1} \right\rfloor_{m_1}$ and $\left\lfloor p_{1_1} \right\rfloor_{m_1}$ cannot hold, since that would imply that $\left\lfloor c_{e_1,n} \right\rfloor_{m_1}$ holds. So in this case, we can conclude (2) since $\left\lfloor w \right\rfloor_{m} = 1_{m_1} \times \left\lfloor w_2 \right\rfloor_{m_2}$ and $w_2$ is $\Psi$-lossless.

Otherwise, $\left\lfloor e_1 \right\rfloor_{m}$ holds. We proceed by case analysis on $\left\lfloor p_{0_1} \right\rfloor_{m_1}$, $\left\lfloor p_{1_1} \right\rfloor_{m_1}$ and $\left\lfloor p_{2_1} \right\rfloor_{m_1}$, as they are mutually exclusive by the premise.
Figure 4. Derived rules

- If \([p_0]_{m_1}\) holds, \(k_1 > 0\) implies
  \[
  \left[ e_{1;e_{1,1};n+1} \right]_{m_1} = \left[ e_{1;e_{1,1};n} \right]_{m_1} \leq \left[ e_{1;e_{1,1};n} \right]_{m_1}
  \]
  which allows us to conclude using the induction hypothesis, since \([w]_{m_1} = [w]_{m_1}\) in this case and \([e_{1;e_{1,1};n}]_{m_1} = \pi_1([w]_{m_1})\).

- If \([p_1]_{m_1}\) holds, we have
  \[
  \left[ e_{1;e_{1,1};n+1} \right]_{m_1} = \left[ e_{1;e_{1,1};1} \right]_{m_1}
  \]
  which allows to conclude using the induction hypothesis.

- If \([p_2]_{m_1}\) holds, we have
  \[
  \left[ e_{1;e_{1,1};n+1} \right]_{m_1} = \left[ e_{1;e_{1,1};1} \right]_{m_1}
  \]
  Note that after the executing while \(e_2 \land p_2\) do \(e_2\)—which is lossless—\(\Psi\) and \(e_1\) still hold while \(e_2\) does not. By the premises of the rule, \(p_2\) must be false so \(p_2\) or \(p_1\) holds on every memory \(m_1\) in the support. By the first two cases with initial memory \(m_1\), we have:
  \[
  \left[ e_{1;e_{1,1};n+1} \right]_{m_1} \leq \pi_1 \left[ w \right]_{m_1'}.
  \]
  We can then conclude:
  \[
  \left[ e_{1;e_{1,1};n+1} \right]_{m_1} \leq \pi_1 \left[ w \right]_{m_1'} \] (linearity)
  \[
  = \pi_1 \left[ w \right]_{m_1'} \] (separable)
  \[
  = \pi_1 \left[ w \right]_{m_1} \] (definition)
  Where the second to last step is because while \(e_2 \land p_2\) do \(e_2\) does not modify \(\pi_1 m\) since \(e_1, e_2\) are separable.

The proof of Eq. (3) follows the same pattern.

Although it is not a primary objective of our work, we briefly comment on completeness of the logic. First, the coupling method is not complete for proving rapid mixing of Markov chains\footnote{Kumar and Ramesh \cite{Kumar} show that the class of causal couplings—which contains all couplings in our logic—are unable to prove rapid mixing for some rapidly-mixing Markov chains \cite{Ramesh,Broder}}. Second, it is not clear that our proof system is complete with respect to hoisting random assignments out of loops.

However, we note that the deterministic fragment of our logic achieves completeness for programs that satisfy a sufficiently strong termination property; the key is that the new rule for while subsumes self-composition for while loops, provided they terminate on all initial memories satisfying the invariant. More precisely, we can prove the following completeness theorem.

**Theorem 8.** Let \(e_1\) and \(e_2\) be separable deterministic programs. If \([\Phi] e_1; e_2 \{ \Psi \}\) is derivable using the rules from Figure 2 then \([\Phi] e_1 \{ \Psi \}\) is derivable. Therefore, \(\times pRHL\) is relatively complete for deterministic programs.

**Proof sketch.** It suffices to prove that if \([\Phi] e_1 \{ \Psi \}\) is derivable using Hoare logic, then

\[
[\Phi] e_1 \{ \Psi \} \quad \text{is derivable. The proof proceeds by induction on the derivation.}
\]
3.4 Convergence from couplings

The fundamental theorem of couplings (Theorem 4) gives a powerful method to prove convergence of random processes. First, we recast it in terms of $\times$pRHL.

Proposition 9. Let $c_1$ and $c_2$ be separable programs and assume that the following judgment is valid:

$$\{ \Phi \} c_1 \{ x_1 = x_2 \} \leadsto c$$

Then for every memory $m$ such that $m \models \Phi$, we have

$$TV(\mu_1, \mu_2) \leq \frac{1}{x_{\#}[c_1]_m}$$

where $\mu_1$, $\mu_2$ are the distributions obtained by sampling $x_1$ from $[c_1]_m$ and $x_2$ from $[c_2]_m$ respectively.

This result is a direct consequence of the soundness of the logic, and allows proving convergence in two parts. First, we use $\times$pRHL to establish a valid post-condition of the form $\Psi \Rightarrow x_1 = x_2$. Second, we prove that for every memory $m$ satisfying some pre-condition, the product program $c$ built from the derivation satisfies:

$$\Pr_{x \leftarrow [c]_m}[\neg \Psi] \leq \beta$$

There are multiple approaches for proving properties of this form—reasoning directly about the semantics of programs; existing formalisms for bounding probabilities and reasoning about expectations (e.g., [37, 38, 39]); program logics for probabilistic programs (e.g., [10, 28, 29]). We will check the property on pen and paper; mechanizing the proofs is left for future work.

4. Application: convergence of Markov chains

We now turn to our first group of examples: proving convergence of probabilistic processes. Suppose we have a probabilistic process on a set $\Omega$ of possible states. At each time step, the process selects the next state probabilistically. Consider two runs of the same program. To ensure that the two copies are separable, we tag all the variables of the first copy with 1, and all the variables of the second copy with 2.

Notation. Throughout this section, we consider two copies of the same program. To ensure that the two copies are separable, we tag all the variables of the first copy with 1, and all the variables of the second copy with 2.

4.1 Simple, symmetric random walk

$x \leftarrow s_1; t \leftarrow 0; l \leftarrow [];$

while $t < T$ do

$r \triangleq \{-1, 1\};$

$x \leftarrow x + r;$

$l \leftarrow x :: l;$

$t \leftarrow t + 1;$

return $x$

Figure 5. Random walk

Our first example is a simple random walk on the integers. Let the state space $\Omega$ be $\mathbb{Z}$. At each step, the process chooses uniformly to move left (decreasing the position by 1) or right (increasing the position by 1). The program $\text{rwalk}$ in Figure 5 implements the process, executed for $T$ steps. The variable $l$ is a ghost variable. While it does not influence the process, it keeps track of the list of sampled values, and will be used to state assertions when we construct the coupling.

Now, consider the random walk started from starting positions $s_1, s_2$. We want to show that the TV-distance between the two distributions on positions decreases as we run for more steps $T$; roughly, the random walk forgets its initial position. It is not hard to see that if $s_1 - s_2$ is an odd integer, then we will not have convergence: at any timestep $t$, the support of one distribution will be on even integers while the support of the other distribution will be on odd integers, so the TV-distance remains 1.

When $s_1 - s_2 = 2k$ is even, we can construct a coupling to show convergence. Barthe et al. [12] used pRHL to couple these random walks by mirroring; informally, the coupled walks make mirror moves until they meet, when they make identical moves to stay equal. Specifically, they show that

$$\{ \Phi \} \text{rwalk}_1 \{ k \in \text{psum}(\text{rev}(l_1)) \Rightarrow x_1 = x_2 \}$$

where $\Phi \triangleq s_1 + s_2 = 2k$, $\text{rev}(l)$ reverses the list, and $\text{psum}(l)$ is the list of partial sums of $l$ (sums over its initial segments). We can lift the judgment to $\times$pRHL

$$\{ \Phi \} \text{rwalk}_1 \{ k \in \text{psum}(\text{rev}(l_1)) \Rightarrow x_1 = x_2 \} \leadsto \text{rwalk}_0$$

where $\text{rwalk}_0$ is the following product program:

$x_1 \leftarrow s_1; x_2 \leftarrow s_2; t_1 \leftarrow 0; t_2 \leftarrow 0; l_1 \leftarrow []; l_2 \leftarrow [];$

while $t_1 < T$ do

if $x_1 = x_2$ then

$(r_1, r_2) \triangleq D_z^\pi(\{-1, 1\})$

else

$(r_1, r_2) \triangleq D_{\text{opp}}(\{-1, 1\})$

$x_1 \leftarrow x_1 + r_1; x_2 \leftarrow x_2 + r_2;$

$l_1 \leftarrow x_1 :: l_1; l_2 \leftarrow x_2 :: l_2;$

$t_1 \leftarrow t_1 + 1; t_2 \leftarrow t_2 + 1;$

return $(x_1, x_2)$

where $\text{opp } x \triangleq -x$.

We briefly sketch the derivation of the product. We start by an application of the [WHILE-S] rule with the invariant

$$\Psi \triangleright k \in \text{psum}(\text{rev}(l_1)) \Rightarrow x_1 = x_2$$

$$\land k \notin \text{psum}(\text{rev}(l_1)) \Rightarrow x_1 - x_2 = 2k - \text{sum}(l_1),$$

where $\text{sum}(l)$ is the sum of the list. Then, we apply a [SEQ] rule (consuming the first random sampling on each side) with intermediate assertion

$$\Xi \triangleq \Psi \land (x_1 = x_2 \Rightarrow r_1 = r_2) \land (x_1 \neq x_2 \Rightarrow r_1 = -r_2)$$

The sub-proof obligation on tails is straightforward, the interesting one is for the random sampling. We start by using the [CASE] rule with $c \triangleq x_1 = x_2$, which introduce the conditional in the product program. If the equality holds, then the two random values are synchronized using the $D_z^{\pi}(\{-1, 1\})$; if not, they are mirrored using $D_{\text{opp}}(\{-1, 1\})$. In our mirror coupling, $k \in \text{psum}(l_1)$ implies that both the have already met, and continue to have the same value.

However, the derivation by itself does not tell us how far the two distributions are, as a function of $T$. To get this information, we will use the probabilistic product construction and the following classical result from the theory of random walks.

Theorem 10 (e.g., [4]). Let $X_0, X_1, \ldots$ be a symmetric random walk on the integers with initial position $X_0 = 0$. Then, for any position $k \in \mathbb{Z}$, the probability that the walk does not reach $k$ within $t$ steps is at most

$$\Pr[X_0, \ldots, X_t \neq k] \leq \frac{ke^{-2}}{\sqrt{\pi t}}.$$
we have
\[
TV([\text{rwalk}]_{m_1}, [\text{rwalk}]_{m_2}) \leq \frac{ke\sqrt{2}}{\pi\sqrt{T}}.
\]

Proof. Conceptually, we can think of the difference \(x_1 - x_2\) as a random walk which increases by 2 with half probability and decreases by 2 with half probability. By applying Theorem 10 to this random walk, we find that in the product program \(c_0\),
\[
Pr[k \notin psum(l_1)] \leq \frac{ke\sqrt{2}}{\pi\sqrt{T}}.
\]
Then, we can conclude by Proposition 9.

4.2 The Dynkin process

Our second example models a process called the Dynkin process. There is a sequence of \(N\) concealed cards, each with a number drawn uniformly at random from \([1, \ldots, 10]\). A player starts at some position in \([1, \ldots, 10]\). Randomly, the player looks at the number at their current position, and moves forward that many steps. For instance, if the player reveals 2 at their current location, then she moves forward two spaces. The player stops when she passes the last card of the sequence. We want to show fast convergence of this process if we start from any two initial positions. In code, the Dynkin process is captured by the program dynkin defined in Figure 6. Here, \(l\) stores the history of positions of the player; this ghost variable will be useful both for writing assertions about the coupling, and for assertions in the product program. Just like for random walks, we can consider the mixing rate of this process, starting from two positions \(s_1, s_2\).

We will couple two runs of the Dynkin process from two starting positions asynchronously: we will move whichever process is behind, holding the other process temporarily fixed. If both processes are at the same position, then they move together.

Figure 6. Dynkin process

Formally, we prove the following \(\times\)pRHL judgment:
\[
\{ T \}
\text{dynkin}_1, \text{dynkin}_2 \quad \{ (l_1 \cap l_2 \neq \emptyset) \Rightarrow x_1 = x_2 \} \Rightarrow \text{dynkin}_0
\]
where \(\text{dynkin}_0\) is the following program:
\[
x_1 \leftarrow s_1; \quad x_2 \leftarrow s_2;
\]
\[
l_1 \leftarrow [x_1]; \quad l_2 \leftarrow [x_2];
\]
\[
\text{while } x_1 < N \land x_2 < N \text{ do}
\]
\[
\text{if } x_1 = x_2 \text{ then}
\]
\[
(r_1, r_2) \leftarrow D^N([1, 10]);
\]
\[
x_1 \leftarrow x_1 + r_1; \quad x_2 \leftarrow x_2 + r_2;
\]
\[
l_1 \leftarrow x_1 :: l_1; \quad l_2 \leftarrow x_2 :: l_2;
\]
\[
\text{else}
\]
\[
\text{if } x_1 < x_2 \text{ then}
\]
\[
r_1 \leftarrow [1, 10];
\]
\[
x_1 \leftarrow x_1 + r_1;
\]
\[
l_1 \leftarrow x_1 :: l_1;
\]
\[
\text{else}
\]
\[
r_2 \leftarrow [1, 10];
\]
\[
x_2 \leftarrow x_2 + r_2;
\]
\[
l_2 \leftarrow x_2 :: l_2;
\]
\[
\text{return } (x_1, x_2)
\]
To couple the two programs, we use the rule [WHILE] with \(k_1 = k_2 = 1\). To control which process will advance, we define:
\[
p_0 \triangleq (x_1 = x_2) \quad p_1 \triangleq (x_1 < x_2) \quad p_2 \triangleq (x_1 > x_2).
\]

The lossless conditions are satisfied since the distance between \(x_1\) and \(x_2\) strictly decreases at each iteration of the loops. For the samplings, when \(p_1\) or \(p_2\) hold we use the one-sided rules for random sampling ([RAND-L] and corresponding [RAND-R]); when \(p_0\) holds, we use the identity coupling.

Theorem 12. Let \(m_1\) and \(m_2\) two memories such that \(m_1(s), m_2(s) \in [1, 10]\), and suppose \(N > 10\). Then:
\[
TV([\text{dynkin}]_{m_1}, [\text{dynkin}]_{m_2}) \leq (\frac{9}{10})^{N/5 - 2}.
\]
The two distributions converge exponentially fast as \(N\) grows.

Proof. In the product program \(\text{dynkin}_0\), we want to bound the probability that \(l_1\) and \(l_2\) are disjoint; i.e., the probability that the two processes never meet. We proceed in two steps. First, it is not hard to show that \(x_1 - x_2 < 10\) is an invariant. Thus, at each iteration, there is a \(1/10\) chance that the lagging process hits the leading process. Second, each process moves at most 10 positions each iteration and we finish when both processes reach the end, so there are at least \(2(\frac{N}{10} - 1) = \frac{9}{5} - 2\) chances to hit. Therefore, in the product we can show
\[
Pr[(l_1 \cap l_2) = \emptyset] \leq (\frac{9}{10})^{N/5 - 2}.
\]
We can then conclude by Proposition 9.

To highlight the quantitative information verified by our approach, we note that the corresponding theorem for random walks (Theorem 11) shows that the total variation distance between two random walks decreases as \(O(1/\sqrt{T})\). In contrast, Theorem 12 shows that the total variation distance between two Dynkin processes converges as \(O(0.9^N)\), giving much faster mixing (exponentially fast instead of polynomially fast).

Remark. The Dynkin process is inspired by the following two-player game. Both players pick a starting position. There is one sequence of random cards that is shared by both players, and players look at the card at their current position and move forward that many spaces. The random cards are shared, so a player samples the card only if the other player has not yet visited the position. If the other player has already landed on the position, the later player looks at the revealed card and moves forward.

While the Dynkin process samples every card that the player lands on, it is not hard to see that the product program exactly models the two-player game. More specifically, the product interleaves the players so that at each turn, the player that is lagging behind makes the next move. By this scheduling, as long as one player is lagging behind, the players have not landed on the same position and so each player lands on unseen cards and draws random samples to reveal. Once the players meet, the product program makes the same move for both players.

For this game, Eq. (4) bounds the probability that the players do not land on the same final position from any two initial positions. This result is the basis of the magic trick called Dynkin’s card trick or the Kruskal count. If one player is the magician and the other player is a spectator, if the spectator starts at a secret position and runs the process mentally, the magician can guess the correct final position with high probability by starting at any position and counting along.

4.3 Path coupling

So far, we have seen how to prove convergence of probabilistic processes by constructing a coupling, reasoning about the probability of the processes not meeting, and applying the coupling theorem. While this reasoning is quite powerful, for more complicated processes it may be difficult to directly construct a coupling that shows fast mixing. For example, it can be difficult to find and reason
about a coupling on the distributions from two states \( s, s' \) if there are many transitions apart in the Markov chain.

To address this problem, Bubley and Dyer \cite{bubley2003glauber} proposed the \textit{path coupling} technique, which allows us to consider just pairs of \textit{adjacent} states, that is states where \( s \) can transition in one step to \( s' \). Roughly speaking, if we can give a good coupling on the distributions from two adjacent states for every pair of adjacent states, then path coupling shows that the state distributions started from two arbitrary states converge quickly.

As the name suggests, path coupling considers paths of states in a probabilistic process. For this to make sense, we need to equip the state space with additional structure. For the basic setup, let \( \Omega \) be a finite set of states and suppose that we have a metric \( d : \Omega \times \Omega \rightarrow \mathbb{N} \). We require that \( d \) is a \textit{path metric}: if \( d(s, s') > 0 \), then there exists \( s'' \neq s, s' \) such that \( d(s, s') = d(s, s'') + d(s'', s') \). Two states are said to be adjacent if \( d(s, s') = 1 \). We will assume that the \textit{diameter} of the state space, i.e. the distance between any two states, is finite: \( \Delta < \infty \). The Markov chain is then defined by iterating a transition function \( f : \Omega \rightarrow \text{Distr}(\Omega) \).

The main idea behind path couplings is that if we can couple the distributions from any two adjacent states, then there exists a coupling for the distributions from two states at an arbitrary distance, constructed by piecing together the couplings along the path. Furthermore, if the expected distance between states contracts under the coupling on adjacent states, i.e., the resulting expected distance is strictly less than 1, then the same holds for the coupling on two states at any distance. More formally, we have the following main theorem of path coupling.

\textbf{Lemma 13} (Bubley and Dyer \cite{bubley2003glauber}). Consider a Markov chain with transition function \( f \) over a set \( \Omega \) with diameter at most \( \Delta \). Suppose that for any two states \( s \) and \( s' \) such that \( d(s, s') = 1 \), there exists a coupling \( \mu \) of \( f(s), f(s') \) such that

\[ E((r, r') - \mu) [d(r, r')] \leq \beta. \]

Then, starting from any two states \( s \) and \( s' \) and running \( t \) steps of the chain, there is a coupling \( \mu' \) of \( f^t(s), f^t(s') \) such that

\[ TV(f^t(s), f^t(s')) \leq (\mu, \mu') [r \neq r'] \leq \beta^t \Delta. \]

This lemma applies for all \( \beta \), but is most interesting for \( \beta < 1 \) when it implies that the Markov chain mixes quickly. With the main theorem in hand, we will show how to verify the conditions for path coupling on two examples from Bubley and Dyer \cite{bubley2003glauber}.

\subsection{Graph coloring: the Glauber dynamics.}

Our first example is a Markov chain to provide approximately uniform samples from the set of colorings of a finite graph; it was first analyzed by Jerrum \cite{jerrum1986polynomial}, our analysis follows Bubley and Dyer \cite{bubley2003glauber}.

Recall that a finite \textit{graph} \( G \) is defined by a finite set of \textit{vertices} \( V \), and a symmetric relation \( E \) relating pairs vertices that are connected by an edge; we will let \( N_G(v) \subseteq V \) denote the set of neighbors of \( v \), i.e. the set vertices that have an edge to \( v \) in \( G \). Let \( C \) be the set of \textit{colors}; throughout, we assume that \( C \) is finite. A \textit{coloring} \( \omega \) of \( G \) is a map from \( V \) to \( C \). A coloring is \textit{valid} (sometimes called \textit{proper}) if all neighboring vertices have different colors; for all \( v' \in N_G(v) \) we have \( \omega(v) \neq \omega(v') \). We write \( \mathcal{V}_C(\omega) \) if \( \omega \) is a valid coloring.

The following program \textit{glauber}(\( T \)) models \( T \) steps of the \textit{Glauber dynamics} in statistical physics:

\[
\begin{align*}
& t \leftarrow 0; \\
& \text{while } t < T \text{ do:} \\
& \quad v \leftarrow V; \quad c \leftarrow C; \\
& \quad \text{if } \mathcal{V}_C(\omega[v \mapsto c]) \text{ then } \omega \leftarrow \omega[v \mapsto c] \\
& \quad t \leftarrow t + 1
\end{align*}
\]

Informally, the algorithm starts from a valid coloring \( \omega \) and iteratively modifies it by sampling uniformly a vertex \( v \) and a color \( c \), recoloring the \( v \) with \( c \) if this continues to be a valid coloring.

We want to measure the statistical distance between two executions of the process starting from two initial colorings \( w_1 \) and \( w_2 \) and run the two natural approaches. The first option is to couple the two copies of glauber directly, analyze the product program and apply Proposition \[P\]. The problem is that when the two colorings are far apart, it is hard to reason about how the processes might meet under a coupling; Jerrum \cite{jerrum1986polynomial} adopted this strategy, but the resulting proof is dense and complex.

The second, far simpler option is to apply path coupling. Here, we build a product for just one iteration of the loop, and it suffices to consider cases where the two initial states are adjacent. This drastically simplifies the coupling and analysis of the product program, so we adopt this approach here. For the sake of clarity, we adapt the transition function so that its output is stored in a fresh variable \( w' \), and call the resulting program \textit{glauber}:

\[
\begin{align*}
& v \leftarrow V; \quad c \leftarrow C; \\
& \text{if } \mathcal{V}_C(\omega[v \mapsto c]) \text{ then } w' \leftarrow \omega[v \mapsto c] \text{ else } w' \leftarrow \omega \\
& \text{Note that glauber}^1: w \leftarrow w'; t \leftarrow t + 1 \text{ is semantically equivalent to the loop body of glauber.}
\end{align*}
\]

To apply the path coupling theorem Lemma \[L\] we need to define a path metric on \( \Omega \) and construct a coupling for the process started from two adjacent states. For the path metric, we define the distance \( d(w_1, w_2) \) as the Hamming distance: the number of vertices where \( w_1 \) and \( w_2 \) provide different colors. We say two states are adjacent if \( d(w_1, w_2) = 1 \); these states differ in the color of exactly one vertex. In order to apply path coupling, we need to find a coupling of the transition function on adjacent states such that the expected distance shrinks. We first build the coupling using \(*\text{pRHL}\). Specifically, we prove

\[
\begin{align*}
& \{d(w_1, w_2) = 1\} \text{ glauber}^1 \text{ glauber}^2 \{d(w_1', w_2') \leq 2\} \sim c_0
\end{align*}
\]

where \( c_0 \) is the following program:

\[
\begin{align*}
& v_1, v_2 \leftarrow \mathcal{D}^s(V); \\
& \text{if } v_1 \in N_G(v_0) \text{ then } c_1, c_2 \leftarrow \mathcal{D}_{\pi_{ab}}(C) \text{ else } c_1, c_2 \leftarrow \mathcal{D}^s(C) \\
& \text{if } \mathcal{V}_C(v_1[v_1 \mapsto c_1]) \text{ then } w_1' \leftarrow v_1[v_1 \mapsto c_1] \text{ else } w_1' \leftarrow v_1 \\\n& \text{if } \mathcal{V}_C(v_2[v_2 \mapsto c_2]) \text{ then } w_2' \leftarrow v_2[v_2 \mapsto c_2] \text{ else } w_2'
\end{align*}
\]

We briefly sketch how to prove the judgment. Note that the two states must agree at all vertices, except at a single vertex \( v_0 \). Let \( w_1(v_0) = a \) and \( w_2(v_0) = b \). First, we couple the vertex sampling with the rule \([\text{RAND}]\) using the identity coupling, ensuring \( v_1 = v_2 \). Then, we use the rule \([\text{CASE}]\) to perform a case analysis on the sampled vertex, call it \( v \). If \( v \) is a neighbor of the differing vertex \( v_0 \), we use the rule \([\text{RAND}]\) and the transposition bijection \( \pi_{ab} : C \rightarrow C \) defined by the clauses:

\[
\begin{align*}
& \pi_{ab}(a) = b \\
& \pi_{ab}(b) = a \\
& \pi_{ab}(x) = x \quad \text{otherwise}
\end{align*}
\]

to ensure that \( c_1 = \pi_{ab}(c_2) \). Otherwise, we use the rule \([\text{RAND}]\) and the identity coupling to ensure \( c_1 = c_2 \). By applying the one-sided rules for conditionals to the left and the right sides ([\text{COND-L}] and [\text{COND-R}]), we can conclude the derivation.

Next, we must reason about the expected value of the distance between \( w_1^t \) and \( w_2^t \) after executing the product program.

\textbf{Lemma 14}. Let \( n = |V| \) and \( k = |C| \), and suppose that the graph \( G \) has degree bounded by \( D \). That is, for any \( v \in V \), there are at most \( D \) vertices \( v' \) such that \( E(v, v') \). If \( k \geq D \), then there is a coupling \( \mu \) of the distributions after running glauber\(^1\) on adjacent states such that

\[
E(\omega_1, \omega_2) \sim \mu [d(\omega_1', \omega_2')] \leq 1 - 1/n + 2D/kn.
\]
As in the previous example, we adapt the loop body to form
\begin{equation}
E_{(w_1, w_2)_{\sim \mu}}[d'] = 0 \cdot Pr[d' = 0] + 1 \cdot Pr[d' = 1] + 2 \cdot Pr[d' = 2]
\end{equation}
where
\begin{equation}
\text{Lemma 15.} \quad 0 = 1 - Pr[d' = 0] + Pr[d' = 2]
\end{equation}
\begin{equation}
\leq 1 - Pr[v_1 = v_0 \land \mathcal{V}_G(w')] + Pr[v_1 \in \mathcal{N}_G(v_0) \land c_1 = b]
\end{equation}
\begin{equation}
\leq 1 - \frac{1}{n} \left( 1 - \frac{D}{k} \right) + \frac{D}{nk} = 1 - \frac{1}{n} + \frac{2D}{nk}.
\end{equation}

where $w' = w_1[v_0 \rightarrow c_1]$. The first equality holds because the distance between the two resulting colorings will be at most 2 by judgment Eq. 2. The second equality holds since $1 = Pr[d' = 0] + Pr[d' = 2]$. The second to last step follows since each vertex has at most D neighbors, so there are at least $k - D$ valid colors at any vertex.

Applying the path coupling lemma (Lemma[13], noting that the diameter is $n$ since there are $n$ vertices, proves that the Glauber dynamics mixes quickly if there are sufficiently many colors $k$.

**Theorem 15.** Consider the Glauber dynamics on $k$ colors with a graph $G$ with $n$ vertices and degree at most $D$, and suppose $k \geq 2D + 1$. Then, for some constant $\beta < 1$,

\begin{equation}
TV([\text{glauber}(T)]_{m_1}, [\text{glauber}(T)]_{m_2}) \leq \beta^T n
\end{equation}

for any two initial memories $m_1$ and $m_2$ containing valid colorings.

This theorem recovers the result by Bubley and Dyer [23]: this is the key step to showing that running Glauber dynamics for a small number of steps and taking a sample is almost equivalent to drawing a uniformly random sample from all proper colorings of the graph.

### 4.3.2 Independent sets: the conserved hard-core model

Our second example is from graph theory and statistical physics, modeling the evolution of a physical system in the conserved hard-core lattice gas (CHLG) model [23]. Suppose that we have a set $P$ of particles, and we have a graph $G$. A placement is a map $w : P \rightarrow V$, placing each particle at a vertex of the graph. We wish to place the particles so that each vertex has at most one particle, and no two particles are located at adjacent vertices; we call such a placement safe and denote it by $\mathcal{S}_G(w)$. For a specific graph, there could be multiple safe placements.

If we want to sample a uniformly random safe placement, we can use a simple Markov chain. We take the state space $\Omega = P \rightarrow V$ to be the set of placements. Again, we take $G$ and $P$ to be finite. We start using a safe initial placement. Each step, we sample a particle $p$ from $P$ and a vertex $v$ from $V$ uniformly at random and try to move $p$ to $v$. If $w[p \rightarrow v]$ is safe, then we make this the new placement; otherwise, we keep the same placement. We can model $T$ steps of this dynamics with the following program chlg($T$):

\begin{algorithmic}
\STATE $t \leftarrow 0$;
\WHILE{$t < T$}
\STATE $p \notin P; v \notin V$;
\IF{$\mathcal{S}_G(w[p \rightarrow v])$} \STATE $w \leftarrow w[p \rightarrow v]$ \STATE $t \leftarrow t + 1$
\ENDIF
\ENDWHILE
\end{algorithmic}

As in the previous example, we adapt the loop body to form chlg*:

\begin{algorithmic}
\STATE $p \notin P; v \notin V$;
\IF{$\mathcal{S}_G(w[p \rightarrow v])$} \STATE $w' \leftarrow w[p \rightarrow v]$ \STATE $w \leftarrow w$
\ENDIF
\end{algorithmic}

Like the graph coloring sampler, we take the path metric on placements and try to find a coupling on the distributions from adjacent initial placements.

\begin{algorithmic}
\STATE $s = |P|$ and $n = |V|$, and suppose that the graph $G$ has degree bounded by $D$. Starting from any two adjacent safe placements $w_1$ and $w_2$, there is a coupling $\mu$ on the distributions after one step such that

\begin{equation}
E_{(w_1, w_2)_{\sim \mu}}[d(w_1', w_2')] \leq \left( 1 - \frac{1}{s} \right) \frac{(3D + 1)}{n}.
\end{equation}

**Proof.** Let chlg$^1_{w_1}$, chlg$^1_{w_2}$ be two copies of the transition function, with variables tagged. Consider two adjacent placements $w_1$ and $w_2$. We will sketch how to couple the transitions.

We use rule [RAND] twice to couple the particle and vertex samplings with the identity coupling, ensuring $p_1 = p_2$ and $v_1 = v_2$. Then, we can apply the one-sided rules for conditionals to the left and the right sides (|COND-L| and |COND-R|) to conclude the following judgment:

\begin{equation}
\{ d(w_1, w_2) = 1 \} \sim c_0,
\end{equation}

where $c_0$ is the following product program:

\begin{equation}
(p_1, p_2) \notin \mathcal{D}^*(P); (v_1, v_2) \notin \mathcal{D}^*(V);
\end{equation}

\begin{equation}
\text{if } \mathcal{S}_C(w_1[p \rightarrow v_1]) \text{ then } w_1' \leftarrow w_1[p \rightarrow v_1] \text{ else } w_1' \leftarrow w_1
\end{equation}

\begin{equation}
\text{if } \mathcal{S}_C(w_2[p \rightarrow v_2]) \text{ then } w_2' \leftarrow w_2[p \rightarrow v_2] \text{ else } w_2' \leftarrow w_2
\end{equation}

Then, we can bound the expected distance between $w_1'$, $w_2'$ in the product program. Let $d' = d(w_1', w_2')$, we have:

\begin{equation}
E_{(w_1, w_2)_{\sim \mu}}[d'(w_1', w_2')]
\end{equation}

\begin{equation}
\leq 1 - Pr[d' = 0] + Pr[d' = 2]
\end{equation}

\begin{equation}
\leq 1 - Pr[p \neq 0 \land \mathcal{S}_C(w_1[p \rightarrow v]) \Rightarrow \mathcal{S}_C(w_2[p \rightarrow v])]
\end{equation}

\begin{equation}
\leq 1 - Pr[p \neq 0 \land \mathcal{S}_C(w_1[p \rightarrow v])]
\end{equation}

\begin{equation}
+ Pr[p \neq 0 \land \neg(\mathcal{S}_C(w_1[p \rightarrow v]) \land \mathcal{S}_C(w_2[p \rightarrow v]))]
\end{equation}

\begin{equation}
\leq 1 - \frac{1}{s} \left( 1 - \frac{(s - 1)(D + 1)}{n} \right) + (s - 1) \left( \frac{2(D + 1)}{sn} \right)
\end{equation}

\begin{equation}
= \left( 1 - \frac{1}{s} \right) \frac{(3D + 1)}{n}.
\end{equation}

Applying the path coupling lemma (Lemma[13]) shows that if we iterate the transition function on two initial placements, the resulting distributions on placements converge quickly.

**Theorem 17.** Consider the conserved lattice gas model with $s = |P|$ particles on a graph $G$ with $n = |V|$ vertices and degree at most $D$, where $s \leq n/3(D + 1) + 1$. Then, for a constant $\beta < 1$,

\begin{equation}
TV([\text{chlg}]_{m_1}, [\text{chlg}]_{m_2}) \leq \beta^T s
\end{equation}

\end{document}
for any two initial memories \( m_1, m_2 \) containing safe placements.

Remark. This theorem is slightly weaker than the corresponding result by Bubley and Dyer \([23]\), who prove rapid mixing under the weaker condition \( s \leq n/2(D + 1) + 1 \). Roughly, they use the maximal coupling on the two transition distributions, giving a tighter analysis and better bound. It is also possible use the maximal coupling in \( \times p \text{RHL} \), but the corresponding specification of the coupling distribution would be proved as part of soundness of the logic, rather than as a property of a probabilistic program.

5. Application: loop optimizations

Program equivalence is one of the original motivations for relational program logics \([17]\). In this section, we demonstrate the effectiveness of our logic using several examples of exact and approximate program equivalence. Our first example is a loop transformation which originates from the literature on parallelizing compilers but also has applications in computer-aided cryptography. Our second example is drawn from the recent literature on approximate computing, and is an instance of loop perforation.

5.1 Loop strip-mining

Loop strip-mining (or loop sectioning) is a transformation that turns a loop into a nested loop. While the transformation originates from literature on parallelizing compilers and is primarily used to take advantage of vectorized instructions, it is also useful for formally proving the computational security of certain cryptographic constructions. The following example, Fig. \([7]\) is inspired from a proof of indifferentiability of the SHA3 hash function \([24]\). Using the rule for while loops, we can prove the following:

\[
\begin{align*}
&\{ x_1 = x_2 \} \quad c_1 \quad \{ x_1 = x_2 \} \quad \leadsto \quad c \quad \\
\end{align*}
\]

The crux of the proof is applying the \([\text{WHILE}]\) rule with \( k_1 = 1 \) and \( k_2 = M \), and \( e = 1 < N \), and \( p_0 = \top \), and \( p_1 = p_2 = \bot \) and an invariant \( \Psi \) which strengthens the assertion \( x_1 = x_2 \) mainly by adding \( l_2 = 1 \times M \). Side conditions using \( p_1 \) and \( p_2 \) are trivial to prove (using the \( \text{FALSE} \) rule) since they have \( \bot \) in hypothesis. It remains to check the premise for \( p_0 \), but we now have two synchronized loops; we can use the \([\text{STRUCT}]\) rule to remove the conditional on \( p_0 \) which is always true in this case.

5.2 Loop perforation

Loop perforation \([44, 51]\) is a program transformation that delivers good trade-offs between performance and accuracy, and is practical in many applications, including image and audio processing, simulations and machine-learning. Informally, loop perforation transforms a loop that performs \( n \) iterations of its body into a loop that performs \( m \) iterations of its body, followed by a simple post-processing statement. Figure \([8]\) shows an example of loop perforation inspired from a financial analysis application, called swaps. In this example, every other loop iteration is skipped, and the post-processing statement simply multiplies by 2 the value \( s \) computed by the optimized loop. As for the previous example, we can prove the following judgment:

\[
\begin{align*}
&\{ \top \} \quad c_1 \quad \{ s_1 = s_2 \} \quad \leadsto \quad c \quad \\
\end{align*}
\]

The product program can be built using the \([\text{WHILE}]\) rule. We use \( e = 1 < 2 \times n, p_0 = \top, p_1 = p_2 = \bot \), and \( k_1 = 2 \) and \( k_2 = 1 \), and the invariant is \( s_1 = 2 \times s_2 \). The invariant allows to show, using the

\[s\]

for simplicity, the programs use an operator \( f \) which takes randomness as an argument (note that the value \( s \) is sampled immediately before the assignment using \( f \)), although in the proof of the SHA3 hash function \( f \) is a procedure call whose body performs random samplings.

<table>
<thead>
<tr>
<th>Nested loop</th>
<th>Single loop</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n_1 = 0 ); ( n_1 &lt; N ) do</td>
<td>( l_2 &lt; N \times M ) do</td>
</tr>
<tr>
<td>( j_1 \leftarrow 0 );</td>
<td>( j_2 \leftarrow l_2 \times M );</td>
</tr>
<tr>
<td>while ( j_1 &lt; M ) do</td>
<td>( r_2 \leftarrow l_2 \times M );</td>
</tr>
<tr>
<td>( l_1 \leftarrow l_1 + M );</td>
<td>( x_2 \leftarrow f(l_2, x_2, r_2) );</td>
</tr>
<tr>
<td>( r_1 \leftarrow \mu );</td>
<td>( l_2 \leftarrow l_2 + 1 );</td>
</tr>
<tr>
<td>( x_1 \leftarrow f(l_1, x_1, r_1) );</td>
<td>( t_2 \leftarrow N );</td>
</tr>
<tr>
<td>( j_1 \leftarrow j_1 + 1 );</td>
<td>( j_2 \leftarrow M );</td>
</tr>
<tr>
<td>( t_1 \leftarrow t_1 + 1 );</td>
<td></td>
</tr>
<tr>
<td>( l_1 \leftarrow N \times M );</td>
<td></td>
</tr>
</tbody>
</table>

Product program:

\( n_1 = 0 \); \( l_2 < N \) do

while \( j_1 < N \) do

\( l_1 \leftarrow 1 \times M + j_1 \);

\( t_2 \leftarrow l_2 / M \); \( r_2 \leftarrow l_2 \times M \);

\( x_2 \leftarrow f(l_2, x_2, r_2) \);

\( t_1 \leftarrow t_1 + 1 \);

\( l_1 \leftarrow N \times M \);


Figure 7. Loop strip-mining

Original program:

\( s_1 \leftarrow 0 \);

for \( (t_1 < 2 \times n, t_1 < t_1 + 1) \) do

\( x_1 \leftarrow \mu \); \( s_1 \leftarrow s_1 + x_1 \);

Perforated program:

\( s_2 \leftarrow 0 \);

for \( (t_2 < 2 \times n, t_2 < t_2 + 1) \) do

\( x_2 \leftarrow \mu \); \( s_2 \leftarrow s_2 + x_2 \);

\( s_2 \leftarrow 2 \times s_2 \);

Product program:

\( s_1 \leftarrow 0 \); \( s_2 < 0 \); \( s_1 \leftarrow 0 \); \( s_2 \leftarrow 0 \);

while \( t_1 < 2 \times n \) do

\( x_1, x_2 \leftarrow D^\mu (\mu) \);

\( s_1 \leftarrow s_1 + x_1 \); \( s_2 \leftarrow s_2 + x_2 \);

\( t_1 \leftarrow t_1 + 1 \);

\( x_1 \leftarrow \mu \); \( s_1 \leftarrow s_1 + x_1 \);

\( t_1 \leftarrow t_1 + 1 \); \( t_2 \leftarrow t_2 + 1 \);

\( s_2 \leftarrow 2 \times s_2 \);


Figure 8. Loop perforation

Using the \([\text{STRUCT}]\) rule, that the loop on \( k \) (denoted by \( c_{1-k_1} \) in \([\text{WHILE}]\)) perform exactly 2 iterations. Using the product, one can also analyze the (probabilistic) accuracy rate of the transformed program, using concentration bounds to achieve a more precise bound.

Finally, in some applications the number of iterations performed by the perforated loop is probabilistic; for instance, the program

\( k \leftarrow \text{factors}(n) \); \( s \leftarrow 0 \);

for \( (i \leftarrow 0, i < n, i \leftarrow i + k) \) do

\( x \leftarrow \mu \); \( s \leftarrow s + x \);

\( s \leftarrow k \times s \);

selects uniformly at random a factor \( k \) of the original number \( n \) of iterations, and performs \( n/k \) iterations. It is possible to relate the original and the perforated loop, using the \([\text{WHILE}]\) rule as before.
5.3 Other optimizations and program transformations

Barthe et al. [6] define an inductive method for building valid product programs, and use their method for validating instances of loop optimizations. Their method combines a rule for each program construction and a rule akin to our [STRUCT] rule. Despite this similarity, the two methods are fundamentally different: their treatment of while loops is restricted to synchronized executions. As a consequence, their structural rule is based on a more advanced refinement relation between programs. Nevertheless, we can reproduce all their examples in our formalism, taking advantage of our more powerful rule for loops.

6. Related work

Relational logics can be seen as a proof-theoretical counterpart of semantics-based relational methods such as logical relations. Under this view, our logic bears strong similarities with proof-relevant logical relations [13]. As for proof-relevant logical relations, we expect that manipulating explicit witnesses rather than existentially quantified can help developing meta-theoretical studies of our logic.

Much of the recent work on product programs and relational logics has been motivated by applications to security and compiler correctness. For instance, Barthe et al. [4] explore self-composition for a variety of programming languages and show that it induces a sound and complete reduction of an information flow policy to a safety property. Independently, Darvas et al. [27] consider self-composition and deductive verification based on dynamic logic, also for verifying information flow policies. Later, Terauchi and Aiken [53] introduce the class of 2-safety properties and show a reduction from 2-safety to safety of the self-composed program. Their reduction is more efficient than self-composition as it selectively applies self-composition or a synchronous product construction akin to cross-products (described below). Further improvements appear in Kovács et al. [35], Müller et al. [46]. In a related work, Beringer and Hofmann [20] observe that one can encode 2-safety properties in standard Hoare logic, provided that assertions are sufficiently expressive to model the denotational semantics of programs. Beringer [19] further refines this approach, by introducing the notion of relational decomposition.

Zaks and Pnueli [52] define a cross-product construction, which is well-suited for reasoning about programs with identical control-flow. Barthe et al. [6] generalize the notion of cross-product by proposing a more general notion of product program which subsumes self-composition and cross-products, and show how it enables validation of common loop optimizations. Specifically, they define an inductive relation for proving that $c$ is a valid product for $c_1$ and $c_2$; informally, their rules closely follow those of our system (for deterministic constructs), except for the general rule for while loops; instead, they use a rule that is closer to the pRHL rule, and a rule akin to our [STRUCT] rule, with a much stronger relationship between programs in order to compensate for the lack of generality of their rule. Barthe et al. [14] carry a more precise study of the relative expressiveness of product program constructions and relational program logics. In a different thread of work, Barthe et al. [6] generalize the notion of product program so that it supports verification of refinement properties (modeled by universal quantification over runs of the first program and existential quantification over runs of the second program), as well as the 2-safety properties (modeled by universal quantification over runs of the first and the second programs). These constructions are focused on non-probabilistic programs. Motivated by applications to differential privacy, Barthe et al. [11] define a specialized product construction from probabilistic programs to deterministic programs, so that the original program is differentially private, provided its deterministic product program satisfies some Hoare specification. To the best of our knowledge, this is the sole product construction that goes from a probabilistic language to a deterministic one.

Benton [17] and Yang [56] were among the first to consider relational program logics that support direct reasoning about two programs. Benton [47] introduces Relational Hoare Logic, proves correctness of several program transformations, and soundly embeds a type system for information flow security into his logic. Yang [56] defines Relational Separation Logic and proves the equivalence between Depth-First Search and the Schorr-Waite algorithm. Barthe et al. [5] develop probabilistic Relational Hoare Logic, and use it for proving computational security of cryptographic constructions. In a follow-up work, Barthe et al. [7] develop an approximate variant of probabilistic Relational Hoare Logic, and verify differential privacy of several algorithms. More recently, Sousa and Dillig [52] propose Cartesian Hoare Logic, an extension of relational Hoare logic to an arbitrary finite number of executions.

Several authors have considered relational logics for higher-order programs. Nanjevik et al. [47] develop a relational logic to reason about information flow properties of a higher-order language with mutable state. Ghani et al. [41] introduce a relational type theory, and a supporting categorical model, for reasoning about parametricity. Barthe et al. [19] propose a relational extension of a subset of the $\Gamma^*$; in a follow-up work, Barthe et al. [13] combine a relational refinement type system with a graded monad which they use for modeling differentially private computations.

There are several works that develop more specialized program logics for analyzing relational properties of programs. For instance, Amtoft et al. [2] introduce independence assertions and a supporting program logic for proving information flow security. In a similar way, Chaudhuri et al. [29] propose a logical approach for proving continuity properties of programs, and Carbin et al. [23] develop a logical approach for reasoning about the reliability of approximate computations.

Further afield, there has been a significant amount of work on semantical methods for probabilistic programs and processes initiated by Kozen [46]. For example, see e.g. [21, 22, 40, 49] for some recent developments. In conjunction with these semantics, research in deductive verification methods for non-relational properties of probabilistic programs is an active area of research; examples include [28, 37, 45, 48] for instance only a few systems.

7. Conclusion and future directions

We have introduced $\times\text{pRHL}$, a new program logic that deepens the connection between probabilistic couplings and relational verification of probabilistic programs in two different ways. First, $\times\text{pRHL}$ broadens the class of couplings supported by relational verification. Second, $\times\text{pRHL}$ derivations explicitly build a probabilistic product program, which can be used to analyze mixing times. We have shown the flexibility of our approach on several examples.

There is ample room for future work. On the theoretical side, it would be interesting to extend $\times\text{pRHL}$ to handle continuous distributions as was recently done by Sato [50] for $\text{apRHL}$. Also, we believe that we are just scratching the surface of probabilistic product programs; there should be many further applications, notably in relationship with path couplings, in domains such as Brownian motion [29], molecular evolution [38], and anonymity [12]. On the more practical side, it would be natural to integrate $\times\text{pRHL}$ in EasyCrypt [2], a proof-assistant used for reasoning about computational security of cryptographic constructions, and currently the main implementation of $\text{pRHL}$. We expect that several proofs of cryptographic constructions can be simplified using the new loop rule, and we are also planning to use the loop rule in an ongoing formalization of indistinguishability of the SHA3 standard for hash functions.
References


We only consider deterministic programs in this section, i.e., programs without random samplings. In that case, the semantic \([s]_m\) of a deterministic command is either 0 if the program does not terminate, or of the form \(1_m\). From that remark, we define the operator \(\llbracket \cdot \rrbracket^\ast\) as follow:

\[
\llbracket s \rrbracket^\ast_m = \begin{cases} m' & \text{if } [s]_m = 1_m, \\ \perp & \text{otherwise} \end{cases}
\]

A while loop while \(e\) do \(s\) is said to terminate certainly under condition \(\Phi\), written \(\Phi \Downarrow\) while \(e\) do \(s\), iff for any \(m\) s.t. \(\Phi(m)\), we have \([\text{while } e \text{ do } s]_m^\ast \neq \perp\).

A \textit{Hoare triple} is a triple of the form \(\{\Phi\} s \{\Psi\}\) where \(\Phi\) and \(\Psi\) are assertions and \(s\) is a deterministic command. A Hoare triple is said to be valid, written \(\vdash \{\Phi\} s \{\Psi\}\), iff for any memory \(m\) s.t. \(\Phi(m)\), either \([s]_m^\ast = \perp\) or \(\Psi([s]_m^\ast)\). Figure 9 gives a sound inference system for Hoare triples: If \(\vdash \{\Phi\} s \{\Psi\}\) is derivable from the rules of Figure 9, then \(\vdash \{\Phi\} s \{\Psi\}\). Moreover, this system is complete for programs that only contain certainly terminating loops.

\[
\begin{array}{c}
\vdash \{\Phi\} \text{skip } \{\emptyset\} \quad \text{[SKIP]} \\
\vdash \{\top\} \text{abort } \{\perp\} \quad \text{[ABORT]} \\
\vdash \Phi[x/c] \quad \text{[ASSIGN]} \\
\vdash \{\Phi \land e\} c_1 \{\Psi\} \quad \text{[COND]} \\
\vdash \{\Phi\} \text{if } e \text{ then } c_1 \text{ else } c_2 \{\Psi\} \\
\vdash \{\Phi \land e\} c \{\Psi\} \quad \text{[WHILE]} \\
\vdash \{\Phi\} \text{while } e \text{ do } c \{\Phi \land \neg e\} \\
\vdash \{\Phi\} c_1 \{\Xi\} \quad \text{[SEQ]} \\
\vdash \Xi \quad \text{[SEQ]} \\
\vdash \{\Phi\} c \{\Psi\} \quad \text{[CONSEQ]}
\end{array}
\]

Figure 9. Hoare Logic Rules for Deterministic Programs