Proving uniformity and independence by self-composition and coupling
Gilles Barthe, Thomas Espitau, Benjamin Grégoire, Justin Hsu, Pierre-Yves Strub

To cite this version:
Gilles Barthe, Thomas Espitau, Benjamin Grégoire, Justin Hsu, Pierre-Yves Strub. Proving uniformity and independence by self-composition and coupling. LPAR 2017 - International Conferences on Logic for Programming, Artificial Intelligence and Reasoning, May 2017, Maun, Botswana. pp.19. hal-01541198

HAL Id: hal-01541198
https://hal.sorbonne-universite.fr/hal-01541198
Submitted on 18 Jun 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.
Proving uniformity and independence
by self-composition and coupling

Gilles Barthe\textsuperscript{1}, Thomas Espitau\textsuperscript{2}, Benjamin Grégoire\textsuperscript{3}
Justin Hsu\textsuperscript{4}, and Pierre-Yves Strub\textsuperscript{5}

\textsuperscript{1} IMDEA Software Institute \textsuperscript{2} Sorbonne Universités, UPMC Paris 6
\textsuperscript{3} Inria \textsuperscript{4} University of Pennsylvania \textsuperscript{5} École Polytechnique

Abstract

Proof by coupling is a classical proof technique for establishing probabilistic properties of two probabilistic processes, like stochastic dominance and rapid mixing of Markov chains. More recently, couplings have been investigated as a useful abstraction for formal reasoning about relational properties of probabilistic programs, in particular for modeling reduction-based cryptographic proofs and for verifying differential privacy. In this paper, we demonstrate that probabilistic couplings can be used for verifying non-relational probabilistic properties. Specifically, we show that the program logic pRHL—whose proofs are formal versions of proofs by coupling—can be used for formalizing uniformity and probabilistic independence. We formally verify our main examples using the EasyCrypt proof assistant.

1 Introduction

Uniformity and probabilistic independence are two of the most useful and commonly encountered properties when analyzing randomized computations. Uniform distributions are a central building block of randomized algorithms. Arguably the simplest non-trivial distribution—the coin flip—is a uniform distribution over two values. Given access to uniform samples, there are known transformations for converting the samples to simulate more complex distributions, like Gaussian or Laplacian distributions. Conversely, turning samples from various non-uniform distributions into uniform samples is an active area of research.

Probabilistic independence is no less useful. The probability of a conjunction of independent events can be decomposed as a product of probabilities of individual events, each which can then be analyzed in isolation. Independent random variables are also needed to apply more sophisticated mathematical tools, like concentration inequalities.

Given these and other applications, it is not surprising that researchers have investigated different methods of reasoning about uniformity and independence. For instance, Pearl and Paz\textsuperscript{18} develop an axiomatic theory based on graphoids for modeling conditional independence in probability theory. However, proving uniformity and independence by program verification remains a challenging task. Most verification techniques for probabilistic programs do not treat these properties as first-class assertions, and rely on reasoning principles that are cumbersome to use. Often, the only way to prove uniformity or independence is to prove exact values for the probability of specific events.

For example, consider a formal system for proving properties of the form $\Pr_{[s], m}[E] = p$, which capture the fact that the event $E$ has probability $p$ in the distribution obtained by executing the randomized program $s$ on some initial memory $m$ (many existing systems use this idea, e.g.\cite{9, 13, 15, 17, 19, 20}). Suppose that we want to prove that a program variable $x$ of some finite type $A$ is uniformly distributed in the output distribution $[s], m$. The only way to show this property is to analyze the probability of each output: for every $a \in A$, prove that $\Pr_{[s], m}[x = a] = \frac{1}{|A|}$. 
For independence, the situation is similar. Assume that we want to prove that the two program variables $x$ and $y$ of respective types $A$ and $B$ are (probabilistically) independent in the output distribution $[s]_m$. This can be done by exhibiting functions $f, g, h$ such that for every $a \in A$ and $b \in B$, we have: $\Pr_{[s]_m} [x = a] = f(a)$, $\Pr_{[s]_m} [y = b] = g(b)$, $\Pr_{[s]_m} [x = a \land y = b] = h(a,b)$. Then, independence between $x$ and $y$ holds by proving that $h(a,b) = f(a) \cdot g(b)$ for every $a \in A$ and $b \in B$.

While these approaches work in theory, they can be laborious in practice. It may be awkward to express the probability of $x = a$, and the functions $f, g$ and $h$ may be difficult to produce. The main contribution of this paper is an alternative method based on probabilistic couplings for proving uniformity and independence. Probabilistic couplings are a classical method for proving sophisticated probabilistic properties (e.g., stochastic dominance, rapid mixing of Markov chains, and more [16, 21, 22]). More recently, couplings have been used to reason about relational properties of probabilistic programs, notably differential privacy [5, 6]. Here we show that uniformity and independence properties can also be verified using coupling, despite being non-relational properties. As a consequence, our verification method inherits the many advantages of reasoning by couplings: compositional reasoning, and no need to reason directly about probabilistic events. Concretely, we show how uniformity and independence can be captured in the relational program logic pRHL [1].

In summary, our main contributions are novel methods to prove uniformity and independence properties of probabilistic programs. We prove the soundness of the methods and demonstrate their usefulness on a class of case studies.

**Detailed Contributions**

**Uniformity.** Suppose we have a program $s$ with a program variable $x$ ranging over a finite set $A$, and we want to show that $x$ is distributed uniformly over $A$ after executing $s$. Rather than computing the probability of $\Pr_{[s]_m} [x = a]$ for each $a \in A$, it suffices to show that the probabilities of any two outputs are equal:

$$\forall a_1, a_2 \in A. \Pr_{[s]_m} [x = a_1] = \Pr_{[s]_m} [x = a_2].$$

Now, we can view uniformity as a relational property: if we consider two runs of $s$, then the probability of $x$ being $a_1$ in the first run should be equal to the probability of $x$ being $a_2$ in the second run. In pRHL, this property is described by the following judgment:

$$\forall a_1, a_2 \in A. \vdash s \sim s : \phi \implies x(1) = a_1 \iff x(2) = a_2$$

where the assertion $\phi$ asserts that the initial states are equal.

**Independence.** Proving probabilistic independence is more involved. We show how to prove independence in two different ways. Assume that we want to prove that the program variables $x$ and $y$ of respective finite types $A$ and $B$ are independent. First, if the distribution of $(x, y)$ is uniformly distributed over $A \times B$, then $x$ and $y$ are independent (and are themselves uniformly distributed). Indeed, assume that for all $a \in A$ and $b \in B$ we have $\Pr_{[s]_m} [x = a \land y = b] = \frac{1}{|A| \cdot |B|}$. Then we have $\Pr_{[s]_m} [x = a] = \sum_{b \in B} \Pr_{[s]_m} [x = a \land y = b] = \frac{1}{|A|}$. A similar argument applies to the probability that $y = b$, from which independence follows. Thus, our first method of proving independence is by reduction to proving uniformity.

This approach is simple to use, but it only applies to proving independence of uniform random variables. A more expressive, but also slightly more complicated approach is to express
probabilistic independence as a property of a modified version of the program, without any requirement on uniformity. More specifically, independence of $x$ and $y$ can be derived from the equality between the probabilities of $x = a \land y = b$ and $x_1 = a \land y_2 = b$, where in the first case the probability is taken over the output of the original program $s$, and in the second case the probability is taken over the output of the program $s_1; s_2$, where $s_1$ and $s_2$ are renamings of $s$ (we call $s_1; s_2$ a self-composition of $s$ [2, 12]). The reason is not hard to see. Since the composed programs operate on disjoint memory, the final combined output distribution models two independent runs of the original program $s$. So, the probability $\Pr_{[s_1; s_2]_{m_1 \cup m_2}}[x_1 = a \land y_2 = b]$—where $m_1 \cup m_2$ is the disjoint union of two copies of $m$—is equal to the product of $\Pr_{[s_1]_{m_1}}[x_1 = a]$ and $\Pr_{[s_2]_{m_2}}[y_2 = b]$. Since $s_1$ and $s_2$ are just renamed versions of the original program $s$, these probabilities are in turn equal to $\Pr_{[s]_m}[x = a]$ and $\Pr_{[s]_m}[y = b]$ in the original program.

Our encoding casts independence as a relational property between a program $s$ and its self-composition $s_1; s_2$, a property which can be directly expressed in pRHL:

$$\forall a \in A, b \in B. \forall s \sim s_1; s_2 : \phi \implies (x(1) = a \land y(1) = b) \iff (x(2) = a \land y(2) = b)$$

where the precondition $\phi$ captures the initial conditions. We show that our approach extends to independence and conditional independence of sets of program variables.

**Outline** Section 2 and Section 3 provide the relevant mathematical background and introduce the setting of our work. Section 4, Section 5 and Section 6 respectively address the case of uniformity, independence, and conditional independence. In each case we demonstrate our method using classic examples of randomized algorithms. We conclude the paper with a discussion of alternative techniques for verifying these properties.

## 2 Mathematical Background

For the sake of simplicity, we restrict ourselves to discrete (countable) sub-distributions.

**Definition 1.** A sub-distribution over a set $A$ is defined by a mass function $\mu : A \to \mathbb{R}^+$, which gives the probability of the unitary events $a \in A$. This mass function must be s.t. $\sum_{a \in A} \mu(a)$ is well-defined and its weight satisfies $|\mu| \triangleq \sum_{a \in A} \mu(a) \leq 1$. In particular, the support of the sub-distribution $\text{supp}(\mu) \triangleq \{a \in A | \mu(a) \neq 0\}$ is discrete. When $|\mu|$ is equal to 1, we call $\mu$ a distribution. We let $D(A)$ denote the set of sub-distributions over $A$. An event over $A$ is a predicate over $A$. The probability of an event $E$ in a sub-distribution $\mu$, written $\Pr_{x \sim \mu}[E]$, is defined as $\sum_{x \in A|E(x)}} \mu(x)$.

When working with sub-distributions over tuples, the probabilistic versions of the usual projections on tuples are called 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 $\pi_1(\mu)(a) \triangleq \sum_{b \in B} \mu(a, b)$ and $\pi_2(\mu)(b) \triangleq \sum_{a \in A} \mu(a, b)$. We are now ready to formally define coupling.

**Definition 2.** Let $A_1$ and $A_2$ be two sets, and let $\Psi \subseteq A_1 \times A_2$. A $\Psi$-coupling for two sub-distributions $\mu_1, \mu_2$ resp. over $A_1$ and $A_2$ is a sub-distribution $\mu \in D(A_1 \times A_2)$ such that $\pi_1(\mu) = \mu_1$ and $\pi_2(\mu) = \mu_2$ and $\text{supp}(\mu) \subseteq \Psi$. We write $\bowtie_{\Psi} (\mu_1 \& \mu_2)$ to denote the existence of a $\Psi$-coupling.

In addition to the general definition, we shall also consider a special case of coupling; specifically, we say that $(\mu_1, \mu_2)$ are $f$-coupled if $f : A_1 \to A_2$ is a bijection such that $\mu_1(x) = \mu_2(f(x))$ for every $x \in A_1$. In this case, we write $f \bowtie (\mu_1 \& \mu_2)$. 

3
We will work with a simple probabilistic imperative language. Probabilistic assignments are of the form \( x \leftarrow g \), which assigns a value sampled according to the distribution \( g \) to the program variable \( x \). The syntax of statements is defined by the grammar:

\[
s ::= \text{skip} \mid \text{abort} \mid x \leftarrow e \mid x \leftarrow g \mid s ; s \mid \text{if} \ e \ \text{then} \ s \ \text{else} \ s \mid \text{while} \ e \ \text{do} \ s
\]

where \( x, e \) and \( g \) respectively range over (typed) variables in \( X \), expressions in \( E \) and distributions in \( D \). To ensure that the set of states is countable, we require that there are finitely many variables \( X \). As usual \( E \) is defined inductively from \( X \) and a set \( F \) of simply typed function symbols. In this paper, distributions used for sampling are either uniform distributions over a finite type \( A \), or the Bernoulli distribution with parameter \( p \), which we denote by \( \text{Bern}(p) \). We assume that expressions and statements are typed in the usual way.

We assume we are given a set-theoretical interpretation for every type and operator of the language. We define a state as a type-preserving mapping from variables to values, and we let \( \text{State} \) denote the set of states. The set of states is equipped with the usual functions for reading and writing a value; we use \( m(x) \) to denote the value of \( x \) in \( m \), and \( m[x := v] \) to denote state update, in this case the state obtained from \( m \) by updating the value of \( x \) with \( v \). One can equip \( D(\text{State}) \) with a monadic structure, using the Dirac distributions \( \delta_x \) for the unit and distribution expectation \( \mathbb{E}_{x \sim \mu}[M(x)] \) for the bind, where

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

The semantics of expressions and distribution expressions is parametrized by a state \( m \), and is defined in the usual way where we require all distribution expressions to be interpreted as proper distributions (sub-distributions with weight 1).

3 Setting

Previous works establish a number of basic facts about couplings, see e.g. Barthe et al. [1, 5]. In particular, one useful consequence of couplings is that they can show that one event has smaller probability than another.

**Lemma 3** (Fundamental lemma of coupling). Let \( E_1 \) and \( E_2 \) be predicates over \( A_1 \) and \( A_2 \), and let \( \Psi \triangleq \{(x_1, x_2) \mid (x_1 \in E_1) \Rightarrow (x_2 \in E_2)\} \). If \( \preceq_\Psi \langle \mu_1 & \mu_2 \rangle \), then \( \Pr_{x_1 \sim \mu_1}[E_1] \leq \Pr_{x_2 \sim \mu_2}[E_2] \).

One can immediately derive a variant of the lemma where \( \Rightarrow \) and \( = \) are used in place of \( \Leftrightarrow \) and \( \leq \) respectively. The following lemma provides a converse to the fundamental lemma of coupling in the special case where we are interested in proving the equality of two distributions.

**Lemma 4.** For every \( \mu_1, \mu_2 \in D(A) \), the following are equivalent:

- \( \mu_1 = \mu_2 \);
- for every \( a \in A \), \( \Pr_{x \sim \mu_1}[x = a] = \Pr_{x \sim \mu_2}[x = a] \);
- for every \( a \in A \), \( \preceq_{\Psi_a} \langle \mu_1 & \mu_2 \rangle \) where \( \Psi_a \triangleq \{(x_1, x_2) \mid x_1 = a \Leftrightarrow x_2 = a\} \);
- \( \preceq_{\Psi_A} \langle \mu_1 & \mu_2 \rangle \) where \( \Psi_A \triangleq \{(x_1, x_2) \mid x_1 = x_2\} \).

We note that the third item (existence of liftings for pointwise equality) is often easier to establish than the last item (existence of lifting for equality), since one can choose the coupling for each possible value of \( a \), rather than showing a single coupling for all values of \( a \).
3.2 Probabilistic Relational Hoare Logic

Probabilistic Relational Hoare Logic (pRHL) is a program logic for reasoning about relational properties of probabilistic programs. Its judgments are of the form $\models s_1 \sim s_2 : \phi \implies \psi,$
where \( s_1 \) and \( s_2 \) are commands and the pre-condition \( \phi \) and the post-condition \( \psi \) are relational assertions, i.e. first-order formulae built over generalized expressions. The latter are similar to expressions, except that each variable is tagged with \((1)\) or \((2)\) to indicate the execution that it belongs to; we call the two executions left and right. Generalized expressions are interpreted w.r.t. a pair \((m_1, m_2)\) of states, where the interpretation of the tagged variables \( x(1) \) and \( x(2) \) are \( m_1(x) \) and \( m_2(x) \) respectively. We write \((m_1, m_2) \vdash \phi\) to denote that the interpretation of the assertion \( \phi \) w.r.t. \((m_1, m_2)\) is valid.

**Definition 7.** A judgment \( \vdash s_1 \sim s_2 : \phi \Rightarrow \psi \) is valid iff for every states \( m_1 \) and \( m_2 \), \((m_1, m_2) \vdash \phi \) implies \( \Phi(\Phi(m_1, m_2) \vdash \psi) \) \( \iff \) \((s_1 \mid m_1) \& (s_2 \mid m_2)\).

Fig. 2 presents the main rules of the logic; see Barthe et al. [1, 7] for the full system. The logic includes two-sided rules, which operate on both programs, and one-sided rules, which operate on a single program (left or right).

The [Conseq] rule is the rule of consequence, and reflects that validity is preserved by weakening the post-condition and strengthening the pre-condition. 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 \( \neg \Xi \) and the other where the pre-condition is strengthened with \( \Xi \).

The [Struct] rule allows replacing programs by provably equivalent programs. The rules for proving program equivalence are given in Fig. 3, and manipulate judgments of the form \( \Phi \vdash c = c' \), where \( \Phi \) is a relational assertion. The first rule ([While-Split]) splits a single loop into two loops (the first running while \( c' \) is true, and the second running for the remaining iterations); this transformation is useful for selecting different couplings in different program iterations. The second rule ([Swap]) reorders two instructions, as long as they modify disjoint variables. This allows us to couple sampling instructions that may come from two different parts of the two programs.

Moving on to the two-sided rules, the [Seq] rule for sequential composition simply reflects the compositional property of couplings. The [Assg] rule is standard. The [Rand] rule informally takes a coupling between the two distributions used for sampling in the left and right programs, and requires that every element in the support of the coupling validates the post-condition. The rule is parametrized by a bijective function \( f \) from the domain of the first distribution to the domain of the second distribution. This bijection gives us the freedom to specify the relation between the two samples when we couple them. The [Cond] rule states that two synchronized if statements can related if their respective branches are also related. The [While] rule is the standard while rule adapted to pRHL. Note that we require the guard of the two commands to be equal—so in particular the two loops must make the same number of iterations—and \( \Phi \) plays the role of the while loop invariant as usual.

The one-sided rules Assg-L, Rand-L, Cond-L and While-L are similar two their two-sided variant, but only operate on the left program. The full system includes mirrored versions of each one-sided rule, for reasoning about the right program.

Throughout the paper, we often assert that the left and the right copies of a state are equal. This is captured by the relational assertion \( \text{EqMem} \underset{\oplus}{\triangleq} \bigwedge_{x \in X} x(1) = x(2) \). We also often assert cross-equality on \( n \)-fold composition of states \( \text{EqMem}^{(p)} \underset{\oplus}{\triangleq} \bigwedge_{x \in X, 1 \leq i \leq p, 1 \leq j \leq q} x^i(1) = x^j(2) \).

## 4 Uniformity

Reasoning about probabilistic programs often requires establishing that a set of program variables (each ranging over a finite type) is uniformly distributed:
While-Split

\[ \Phi \vdash \text{while } e \text{ do } s \equiv \text{while } e \land e' \text{ do } s ; \text{while } e \text{ do } s \]

Swap

\[ \frac{\text{var}(s_1) \cap \text{var}(s_2) = \emptyset}{\Phi \vdash s_1 ; s_2 \equiv s_2 ; s_1} \]

Figure 3: Equivalence rules (selection)
Definition 8. A set $X = \{x_1, \ldots, x_n\}$ of program variables of finite types $A_1, \ldots, A_n$ is uniformly distributed in a distribution $\mu \in \mathbb{D}(\text{State})$ iff for every $(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n$:

$$\Pr_{\mu} \left[ \bigwedge_{1 \leq i \leq n} x_i = a_i \right] = \prod_{1 \leq i \leq n} \frac{1}{|A_i|}$$

Note that the definition of uniformity (and as we will see in later sections, the definition of independence) naturally extends to sets of expressions, and so do our characterizations.

4.1 Characterization

The following proposition characterizes uniformity in terms of couplings.

Proposition 9 (Uniformity by coupling). Let $X = \{x_1, \ldots, x_n\}$ be a set of variables of respective finite types $A_1, \ldots, A_n$. For every program $s$, the following are equivalent:
1. for every state $m$, $X$ is uniformly distributed in $[s]_m$;
2. for every two tuples $(a_1, \ldots, a_n), (a'_1, \ldots, a'_n) \in A_1 \times \cdots \times A_n$, we have

$$\models s \sim s : \text{EqMem} \implies \left( \bigwedge_{1 \leq i \leq n} x_i(1) = a_i \right) \iff \left( \bigwedge_{1 \leq i \leq n} x_i(2) = a'_i \right).$$

Proof. [1. $\implies$ 2.] Let $m$ be a memory and assume that $X$ is uniformly distributed in $[s]_m$. Let $(a_1, \ldots, a_n), (a'_1, \ldots, a'_n) \in A_1 \times \cdots \times A_n$. We denote by $f : \text{State} \to \text{State}$ the bijection defined by

$$f(m) = m[x_i \leftarrow a'_i]_{1 \leq i \leq n} \text{ if } \forall i. m[x_i] = a_i$$

$$f(m) = m[x_i \leftarrow a_i]_{1 \leq i \leq n} \text{ if } \forall i. m[x_i] = a'_i$$

$$f(m) = m \text{ otherwise.}$$

Let $\eta \in \mathbb{D}(\text{State} \times \text{State})$ be the distribution defined by $\eta(m_1, m_2) = [s]_m(m_1)$ if $m_2 = f(m_1)$, and $\eta(m_1, m_2) = 0$ otherwise. We prove that $\eta$ is a $\Psi$-coupling for $[s]_m$, where

$$\psi \triangleq \left( \bigwedge_{1 \leq i \leq n} x_i(1) = a_i \right) \iff \left( \bigwedge_{1 \leq i \leq n} x_i(2) = a'_i \right).$$

Regarding the marginals, we have:

$$\pi_1(\eta)(m_1) = \sum_{m_2} \eta(m_1, m_2) = \eta(m_1, f(m_1)) = [s]_m(m_1)$$

$$\pi_2(\eta)(m_2) = \sum_{m_1} \eta(m_1, m_2) = \eta(f^{-1}(m_2), m_2) = [s]_m(f^{-1}(m_2))$$

the last equality being a consequence of $X$ being uniformly distributed in $[s]_m$. Moreover, for $(m_1, m_2) \in \text{supp}(\eta)$, we have $m_2 = f(m_1)$. Thus, $m_1[x_i] = a_i$ if $m_2[x_i] = a'_i$, and $m_1, m_2 \models \Psi$.

[2. $\implies$ 1.] Let $(a_1, \ldots, a_n), (a'_1, \ldots, a'_n) \in A_1 \times \cdots \times A_n$ and assume that $\models s \sim s : \text{EqMem} \implies \Psi$, where $\Psi$ is defined as in the previous case. Since $m, m \models \text{EqMem}$, by Lemma 3 we have:

$$\Pr_{[s]_m} \left[ \bigwedge_{1 \leq i \leq n} x_i = a_i \right] = \Pr_{[s]_m} \left[ \bigwedge_{1 \leq i \leq n} x_i = a'_i \right],$$

showing that $X$ is uniform in $[s]_m$. \qed
By expressing uniformity as a coupling property, we can use pRHL to prove uniformity. To demonstrate the technique, we consider classical examples from the theory of randomized algorithms.

### 4.2 Simulating a Fair Coin

This example considers a process for simulating a fair coin using a biased coin. The idea is simple: 1) toss the coin twice; 2) if the two outcomes differ, return the value of the first coin; 3) if the two outcomes match, repeat from step 1. The algorithm does not require the bias of the coin to be known, as long as it is some constant bias and there is positive probability of returning 0 and 1. This process can be modelled by the program \( s \) from Fig. 4, where \( 0 < p < 1 \) is a real parameter modeling the probability of the biased coin to return 0 (tail). Our goal is to establish the trivial judgment \( \{ \top \} s \{ \top \} \) and the following pRHL judgment:

\[
\models s \sim : \top \implies x(1) \iff \neg x(2)
\]

By the fundamental lemma of coupling, this implies that \( \Pr_{[x]_m}[x = 1] = \Pr_{[x]_m}[x = 0] \), and hence that \( x \) is uniformly distributed upon termination. The proof proceeds by establishing the following invariant:

\[
x(2) = \text{if } x(1) = y(1) \text{ then } y(2) \text{ else } \neg x(1)
\]

Validity of the invariant entails that the desired postcondition holds when the program exits, as the invariant and the negation of the loop guard both hold. The invariant holds when entering the loop, so we only need to prove that it is preserved by the loop body. The proof proceeds as follows: first, we swap the two random assignments on the right, leading to the judgment:

\[
\models (x \leftarrow \text{Bern}(p); \ y \leftarrow \text{Bern}(p)) \sim (y \leftarrow \text{Bern}(p); \ x \leftarrow \text{Bern}(p)) : \phi' \implies \phi
\]

where \( \phi \) denotes the loop invariant and \( \phi' \) denotes its strengthening by the loop guard—we do not need the precondition, since the values are freshly sampled in the body. Next, we apply the \[\text{Rand}\] rule twice, with the identity bijection. The required pre-condition

\[
\forall v_1, v_2, v_2 = (\text{if } v_1 = v_2 \text{ then } v_1 \text{ else } \neg v_1)
\]

is clearly true.

### 4.3 Cyclic Random Walk

Consider a random walk over a cyclic path composed of \( n \) nodes labeled 0, 1, \ldots, \( n - 1 \): starting from position 0, at each step, we flip a fair coin over \( \{-1, 1\} \) and update the position accordingly to the result of the coin flip. To take into account that we are on a cyclic structure, all arithmetical operations are in the cyclic ring \( \mathbb{Z}/n\mathbb{Z} \)—i.e. performed modulo \( n \). At each iteration, when moving between two contiguous positions over the circle, we consider that the random walk visited the arc between the two nodes. We want to show that the last visited arc is uniformly distributed. Fig. 5 (left) gives a graphical representation of the random walk, where \( c \) is the random walk position and the dashed arc is the last visited arc when \( c \) moved from 0 to 1.
This process can be seen as a simple version of an algorithm that samples a uniformly random spanning tree on a graph—when the graph is a cycle, a spanning tree visits all but one of the edges. While Broder [8] analyzes the general problem, we can verify uniformity for the cyclic random walk with couplings.

The proof proceeds as follows. We imagine executing two random walks, from the same initial position. The goal is to couple the walks so that \((a,a+1)\) is the last arc in the first walk if and only if \((b,b+1)\) is the last arc in the second walk. If we can show this property for all \(a,b\), then this coupling argument shows that any two arcs have the same probability of being the last arc, hence the last arc must be uniformly distributed.

To describe the coupling informally, we first execute asynchronously the two random walks until they eventually synchronize respectively on the arcs \((a,a+1)\) and \((b,b+1)\). At that point, we are in one of the following cases: either the random walks synchronize on the same side of the arcs \((a,a+1)\) and \((b,b+1)\), or they synchronize on opposite sides. (These cases are depicted on the left diagrams above, where the arc we want to synchronize on is dashed.) From that point, we execute the two processes resp. in lock-step (if they synchronized on the same side) or anti-lock-step (if they did not).

At some point, both processes will visit the other side of the arcs \((a,a+1)\) and \((b,b+1)\), and since they execute in (anti)-lock-step, these events will occur synchronously.

At that point, either the processes finished their walk and they resp. return the arcs \((a,a+1)\) and \((b,b+1)\) as their result (case (i) of the right diagram above), or they have other nodes to visit and so they will not resp. return the arcs \((a,a+1)\) and \((b,b+1)\) (case (ii) of the same diagram).

We now detail the formal proof. Consider the program of Fig. 5, where all arithmetical operations are done modulo \(n\). This algorithm instruments the random walk with two points \(f\) and \(l\) representing the range \([f,l]\) (using clockwise ordering) of all the points that have been visited by the walk. When all nodes of the cycle have been visited (i.e. when \(l+1 = f\)), the arc between \(l\) and \(l+1\) is the only arc that has not been visited by the walk. Let \(s\) be the
program of Fig. 5 and \( s' \) the loop body of the single loop of \( s \). We want to show that the final
arc \( ret \)—the only arc that has not been marked—is uniformly distributed among all arcs. This
follows by the judgment:

\[
\forall a, b \in \mathbb{Z}/n\mathbb{Z}, \therefore s \sim s : \top \implies \text{ret}(1) = (a, a + 1) \iff \text{ret}(2) = (b, b + 1).
\]

First, we make use of the loop splitting equivalence rule ([While-Split]) to transform the
main loop into three pieces. In the left program:

\[
\begin{align*}
\text{while } (|v| < n \land a, a + 1 \notin [f, l]) & \text{ do } s'; \\
\text{while } (|v| < n \land (a, a + 1 \in [f, l])) & \text{ do } s'; \\
\text{while } (|v| < n) & \text{ do } s'
\end{align*}
\]

where \([f, l]\) represent the range \( f, f + 1, \ldots, l \). We use a similar transformation on the right
program, with \( b \) in place of \( a \). To carry out the proof, we first use the one-sided loop rules
([While-L] and the corresponding version [While-R]) on the first loops of the left and right
programs. This part of the proof correspond to the walks synchronization as described above.
By a straightforward loop invariant, we can show that

\[
\Phi \land P(a)(1) \land P(b)(2)
\]

holds after the first loops, where \( P(x) \triangleq (x \in [f, l] \lor (x + 1) \in [f, l]) \) and \( \Phi \triangleq \forall i \in \{1, 2\}, (c \in [f, l])(i) \) indicates that the current positions \((c(1), c(2))\) are contained in the range of visited arcs. Next, we show that after the two second loops the following relational invariant is satisfied:

\[
(a, a + 1 \in [f, l])(1) \land (b, b + 1 \in [f, l])(2) \land (l(1) = a \iff l(2) = b)
\]

After the second loop, there are two cases for the third loop. If \( l(1) = a \), we have \( l(2) = b \), \( f(1) = a + 1 \) (since \( a + 1 \) is visited in \( 1 \)) and \( f(2) = b + 1 \). In this case, which corresponds to the case (i) of the last diagram, the third loops both exit immediately and the random walks resp. return the arcs \((a, a + 1)\) and \((b, b + 1)\). Otherwise, we have \( l(1) \neq a \) and \( l(2) \neq b \), and we can show, using the rules [While-L] and [While-R], that \( l(1) \) (resp. \( l(2) \)) will never be set to \( a \) (resp. \( b \)). In this case, which corresponds to the case (ii) of the last diagram, we can show that the walks resp. return arcs distinct from \((a, a + 1)\) and \((b, b + 1)\).

We now focus on the second loops, relating them with the two-sided variant of the [While]
rule. The particular coupling we choose will depend on the current positions in the two sides at
the start of the second loops. If \( a \in [f, l] \) and \( b \in [f, l] \) then we have \( l(1) = a \) and \( l(2) = b \)
(since \( a + 1 \notin [f, l] \)) and we couple the walks to make identical moves. In that case, the key
part of the loop invariant is:

\[
\land \left\{ \Phi \land (a \in [f, l])(1) \land (b \in [f, l])(2) \\
\quad \land (c(1) - a = c(2) - b) \\
\quad \land (l(1) = a \iff l(2) = b) \right\}
\]

The first line enforces some structural invariant and the second line enforces that both walks
make identical moves relative to \( a \) and \( b \). The main difficulty is to show that both loops are
synchronized. Note that there are two reasons the loop may exit. If \( l \) has been incremented,
then the increment will be done on both side. Otherwise, if \( f \) has been decremented to \( a + 1 \),
then we have \( c(1) = f(1) = a + 2 \), so \( c(1) - a = c(2) - b = 2 \) and \( c(2) = b + 2 \) and the right
loop will also decrement \( f \) to \( b + 1 \). The case \( a + 1 \in [f, l] \) and \( b + 1 \in [f, l] \) is very similar,
by reversing the roles of \( f \) and \( l \). The remaining two cases, \( a + 1 \in [f, l] \) and \( b \in [f, l] \) or
\( a \in [f, l] \) and \( b + 1 \in [f, l] \) is similar except that we force the walks to be execute in
anti-lock-step. Using the rule [Case], we put together these four cases and we conclude by
application of the rule for sequence.
4.4 Ballot Theorem

So far, we have shown how couplings can be used to prove that a set of program variables is uniformly distributed. Couplings can also be used for showing that two events have the same probability, such as in the following example.

**Example 10** (Ballot Theorem). Assume that voters must choose between two candidates $A$ and $B$. The outcome of the vote is $n_A$ votes for $A$ and $n_B$ votes for $B$, with $n_A > n_B$. Assuming that the order in which the votes are cast is uniformly random, the probability that $A$ is always strictly ahead in partial counts is $(n_A - n_B)/(n_A + n_B)$.

The process can be formalized by the program from Fig. 6. Here we use the list $l$ to store intermediate results. Using $l_i$ to denote the $i$-th element of the list $l$, the Ballot Theorem is captured by the statement:

$$\forall n_A, n_B. n_A > n_B \implies \Pr_{[s]_m} \left[ \bigwedge_{1 \leq i \leq n} l_i \neq 0 \mid x_A = n_A \land x_B = n_B \right] = \frac{n_A - n_B}{n_A + n_B}.$$ 

![Figure 6: Ballot theorem](image)

It follows from the properties of coupling that for every $n_A$ and $n_B$ such that $n_A > n_B$, $\Pr_{[s]_m} [l_1 \cdot l_n > 0 \land \phi \land l_n = k] = \Pr_{[s]_m} [l_1 \cdot l_n < 0 \land \phi \land l_n = k]$. In terms of conditional probabilities, we have $\Pr_{[s]_m} [l_1 \cdot l_n > 0 \land \phi \mid \psi] = \Pr_{[s]_m} [l_1 \cdot l_n < 0 \land \phi \mid \psi]$. Now observe that any sequence that starts with a vote to $B$ (i.e. the loser) is necessarily bad. Therefore, $\Pr_{[s]_m} [l_1 \cdot l_n < 0 \land \phi \mid \psi] = \Pr_{[s]_m} [l_1 \cdot l_n < 0 \mid \psi]$. By the above and elementary properties of conditional independence:

$$\Pr_{[s]_m} [\phi \mid \psi] = \Pr_{[s]_m} [l_1 \cdot l_n > 0 \land \phi \mid \psi] + \Pr_{[s]_m} [l_1 \cdot l_n < 0 \land \phi \mid \psi]$$

$$= 2 \cdot \Pr_{[s]_m} [l_1 \cdot l_n < 0 \mid \psi].$$

Note that the probability in the right-hand side of the last equation represents the probability that the first vote goes to the loser, conditional on $\psi$. This turns out to be exactly $\frac{n_B}{n_A + n_B}$, so we conclude that $\Pr_{[s]_m} [\phi \mid \psi] = 2 \cdot \frac{n_B}{n_A + n_B}$ or equivalently $\Pr_{[s]_m} [-\phi \mid \psi] = \frac{2n_A - n_B}{n_A + n_B}$ as desired.

We now turn to the proof of the pRHL judgments. By symmetry it suffices to consider the first judgment. Using the rule of consequence and the elimination rule for universal quantification, it suffices to prove for every $i$:

$$\vdash s \sim s : \top \implies l_1(1) \cdot l_n(1) > 0 \land l_i(1) = 0 \land \psi(1) \Rightarrow l_1(2) \cdot l_n(2) < 0 \land l_i(2) = 0 \land \psi(2).$$
We couple the samplings of $x$ using the negation function until $|l| = i$, and then with the identity bijection. This establishes the following loop invariant, from which we can conclude:

$$
(\forall j \leq i. l_j(1) = -l_j(2)) \land l_i(1) = l_i(2) = 0 \land (\forall j > i. l_j(1) = l_j(2)).
$$

## 5 Independence

We now turn to characterizing probabilistic independence using couplings. We focus on probabilistic independence of program variables, a common task when reasoning about randomized computations. In our setting, the textbook definition of probabilistic independence can be cast as follows:

**Definition 11.** A set $X = \{x_1, \ldots, x_n\}$ of program variables of types $A_1, \ldots, A_n$ is probabilistically independent in a distribution $\mu \in \mathbb{D}(\text{State})$ iff for every $(a_1, \ldots, a_n) \in A_1 \times \ldots \times A_n$:

$$
\Pr_{\mu} \left[ \bigwedge_{1 \leq i \leq n} x_i = a_i \right] = \prod_{1 \leq i \leq n} \Pr_{\mu} [x_i = a_i].
$$

### 5.1 Characterization

Our first characterization of independence is based on the observation that uniformity entails independence.

**Fact 12** (Independence from uniformity). From every state $m$, if $X$ is uniformly distributed in $\llbracket s \rrbracket_m$ then $X$ is independent in $\llbracket s \rrbracket_m$.

This observation enables proving independence by coupling, in the special case where variables are uniform and independent. For the general case, we will use an alternative characterization based on self-composition.

**Proposition 13** (Independence by coupling). The following are equivalent:

1. for every state $m$, $X$ is independent in $\llbracket s \rrbracket_m$;
2. the following judgment, between a single copy of the program on the one hand and a $n$-fold copy on the other hand, is derivable for every $(a_1, \ldots, a_n) \in A_1 \times \ldots \times A_n$:

$$
\models s \sim s^{(n)} : \text{EqMem}^{(1), (n)} \Rightarrow \bigwedge_{1 \leq i \leq n} x_i(1) = a_i \iff \bigwedge_{1 \leq i \leq n} x^i(2) = a_i.
$$

**Proof.** The validity of the universally quantified $\text{pRHL}$ judgment is equivalent to the following statement: for every $a_1, \ldots, a_n$ and $n$-fold copy $m^{(n)}$ of some initial state $m$,

$$
\Pr_{\llbracket s \rrbracket_m} \left[ \bigwedge_{1 \leq i \leq n} x_i = a_i \right] = \Pr_{\llbracket s^{(n)} \rrbracket_m^{(n)}} \left[ \bigwedge_{1 \leq i \leq n} x^i = a_i \right] = \prod_{1 \leq i \leq n} \Pr_{\llbracket s \rrbracket_m} [x_i = a_i].
$$

The last equality comes from the property of $n$-fold self-composition (Proposition 6).

### 5.2 Pairwise Independence of Bits

Our first example is a well-known algorithm for generating $2^n$ pairwise independent bits. The algorithm first samples $n$ independent bits $b_1 \ldots b_n$, and then defines for every subset $X \subseteq \{1, \ldots, n\}$ the bit $z_X = \bigoplus_{i \in X} b_i$. 

13
We can prove pairwise independence of the computed bits, i.e. for every \( X \neq Y \), \( z_X \) and \( z_Y \) are independent. Since there are \( 2^n \) subsets of \( \{1, \ldots, n\} \), this gives us \( 2^n \) pairwise independent bits constructed from \( n \) independent bits. The algorithm is encoded by the program \( s \) in Fig. 7, where \( \text{bits} \{0, \ldots, 2^n - 1\} \) to a subset in \( \mathcal{P}(\{1, \ldots, n\}) \) of positions that are 1 in the binary representation, and for \( i = a \) to do \( s \) is usual syntactic sugar for while loop with an incrementing counter \( i \).

By our characterization based on self-composition, pairwise independence of \( z_j \) and \( z_{j'} \) for every \( j \neq j' \) is equivalent to the (universally quantified) \( \text{pRHL} \) judgment

\[
\vdash s \sim s_1; s_2 : \top \implies z_j(1) = a \land z_{j'}(1) = a' \iff z_j(2) = a \land z_{j'}(2) = a'.
\]

Since \( j \neq j' \), the two sets \( \text{bits}(j) \) and \( \text{bits}(j') \) must differ in at least one element. Let \( k_0 \) be the smallest element in which they differ. Without loss of generality, we can assume that \( k_0 \notin \text{bits}(j) \) and \( k_0 \in \text{bits}(j') \). The crux of the proof is to establish the following judgment:

\[
\vdash s_1 \sim s_r : \top \implies z(1) = a \land z'(1) = a' \iff z(2) = a \land z''(2) = a'
\]

where \( z = \bigoplus_{k \in \text{bits}(j)} b_k \), \( z' = \bigoplus_{k \in \text{bits}(j')} b_k \) and \( z'' = \bigoplus_{k \in \text{bits}(j')} b'_k \) and

\[
\begin{align*}
s_1 \triangleq & \text{for } i \in [1 \ldots n] \setminus k_0 \text{ do } b_i \triangleq \{0, 1\}; b_k \triangleq \{0, 1\} \\
s_r \triangleq & \text{for } i \in [1 \ldots n] \setminus k_0 \text{ do } b_i \triangleq \{0, 1\}; b'_i \triangleq \{0, 1\}; b_{k_0} \triangleq \{0, 1\}; b'_{k_0} \triangleq \{0, 1\}.
\end{align*}
\]

This is proved by coupling the variables of the two programs in an appropriate way. We couple the random samplings as follows:

- for every \( k \neq k_0 \), we couple \( b_k(1) \) and \( b_k(2) \) using the identity sampling;
- we use the \( \text{RND-R} \) rule for \( b'_k(2) \) for every \( k \neq k_0 \);
- we couple \( b_{k_0}(1) \) and \( b'_{k_0}(2) \) with the bijection which ensures

\[
b_{k_0}(1) \oplus \left( \bigoplus_{k \in \text{bits}(j') \setminus \{k_0\}} b_k(1) \right) = b'_{k_0}(2) \oplus \left( \bigoplus_{k \in \text{bits}(j') \setminus \{k_0\}} b'_k(2) \right).
\]

Putting everything together, the final proof obligation follows from the algebraic properties of \( \oplus \).

### 5.3 \( k \)-wise Independence

The previous example can be generalized to achieve \( k \)-wise independence for general \( k \). Suppose we wish to generate \( n \) random variables that are \( k \)-wise independent. We will work in \( \mathbb{Z}/p\mathbb{Z} \), the field of integers modulo a prime \( p \), such that \( k \leq p \). Let \( a_0, \ldots, a_{k-1} \) be drawn uniformly at random from \( \mathbb{Z}/p\mathbb{Z} \) and define the family of random variables for every \( m \in \{1, \ldots, n\} \):

\[
x_m = \sum_{j=0}^{k-1} a_j \cdot m^j,
\]

where we take \( 0^0 = 1 \) by convention. The corresponding code is given in Fig. 8. Then, we can show that any collection of \( k \) distinct variables \( \{x_i\} \) is independent.
for $i = 1 \text{ to } n$ do
  $a_i \leftarrow Z/p\mathbb{Z}$;
for $m = 0 \text{ to } n - 1$ do
  $x_m \leftarrow 0$;
for $j = 0 \text{ to } k - 1$ do
  $x_m \leftarrow a_j \cdot m^j$;

Figure 8: $k$-wise independence

For simplicity, we will show that the first $k$ elements $x_0, \ldots, x_{k-1}$ are uniform, and hence independent. Let $v_0, \ldots, v_{k-1} \in Z/p\mathbb{Z}$ be arbitrary elements of the field. Then the probability that $(x_0, \ldots, x_{k-1}) = (v_0, \ldots, v_{k-1})$ is equal to $p^{-k}$. Indeed, the equations

\[
\begin{align*}
  v_0 &= a_0 \\
  \vdots \\
  v_{k-1} &= \sum_{j=0}^{k-1} a_j \cdot (k-1)^j
\end{align*}
\]

define a system of linear equations with variables $a_0, \ldots, a_{k-1}$. By basic linear algebra, the system of equations has a unique solution for the variables $a_0, \ldots, a_{k-1}$, which we denote $(v_0^*, \ldots, v_{k-1}^*)$. Now consider the $\PrHL$ judgment that establishes uniformity:

$\vdash s \sim s : \top \implies x_0(1) = v_0 \land \cdots \land x_{k-1}(1) = v_{k-1} \iff x_0(2) = w_0 \land \cdots \land x_{k-1}(2) = w_{k-1}$

By applying (relational) weakest precondition on the deterministic fragments of the program, the judgment is reduced to

$\vdash s \sim s : \top \implies a_0(1) = v_0^* \land \cdots \land a_{k-1}(1) = v_{k-1}^* \iff a_0(2) = w_0^* \land \cdots \land a_{k-1}(2) = w_{k-1}^*$

We then repeatedly apply the rule for random sampling, with the permutation on $Z/p\mathbb{Z}$ that exchanges $(v_1^*, w_1^*)$.  

6 Conditional Independence

Finally, we consider how to show conditional independence. Recall that the conditional probability $\Pr_{x \sim \mu} [A \mid B]$ is defined when $\Pr_{x \sim \mu} [B] \neq 0$ and satisfies $\Pr_{x \sim \mu} [A \mid B] \triangleq \frac{\Pr_{x \sim \mu} [A \land B]}{\Pr_{x \sim \mu} [B]}$.

**Definition 14.** Let $X = \{x_1, \ldots, x_n\}$ be a set of program variables of types $A_1, \ldots, A_n$ and let $E$ be an event. We say that $X$ is independent conditioned on $E$ in a distribution $\mu \in \mathbb{D}(\text{State})$ iff for every $(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n$:

$$
\Pr_{\mu} \left[ \bigwedge_{1 \leq i \leq n} x_i = a_i \mid E \right] = \prod_{1 \leq i \leq n} \Pr_{\mu} [x_i = a_i \mid E].
$$

(For this definition to make sense, we are implicitly assuming that $\Pr_{\mu} [E] \neq 0$.)

1Let the Vandermonde matrix $V(1, \ldots, k-1) = (i^{j-1})_{i,j}$ be

$$
V(1, \ldots, k-1) \cdot (a_0, \ldots, a_{k-1})^T = (v_0, \ldots, v_{k-1})^T.
$$

The system of equations has a unique solution if and only if the matrix $V(1, \ldots, k-1)$ is invertible in the space of matrices over $Z/nZ$, which happens if and only if its determinant is non-zero mod $n$. Expanding,

$$
\det(V(1, \ldots, k-1)) = \prod_{i \neq j} (i - j) = \prod_{i=2}^{k-1} i!
$$

Note that $p$ does not divide the determinant by Gauss’ lemma, since $n$ can’t divide any of the terms $i!$ for any $i < n$. Therefore, the system of equations has a unique solution.
The following lemma unfolds the definition of conditional independence and is useful for the characterization of the next section.

**Lemma 15.** A set of variables $X$ is independent conditioned on an event $E$ in $\mu$ iff for every $a_1 \in A_1, \ldots, a_n \in A_n$:

$$
\Pr_\mu \left[ \bigwedge_{1 \leq i \leq n} x_i = a_i \land E \right] : (\Pr_\mu [E])^{n-1} = \prod_{1 \leq i \leq n} \Pr_\mu [x_i = a_i \land E].
$$

### 6.1 Characterization

The characterization of independence based on self-composition can be extended as follows.

**Proposition 16** (Conditional independence by coupling). The following are equivalent:

1. for every state $m$, $X$ is independent conditioned on $E$ in $[s]_m$;
2. $\vdash s^{(n)} \sim s^{(n)} : \text{EqMem}^{(n),(n)} \implies (\phi_1 \land E^{(1)}) \iff (\phi_2 \land E^{(2)})$ where $E \triangleq \bigwedge_{1 \leq i \leq n} E^i$,

$$
\phi_1 \triangleq \bigwedge_{1 \leq i \leq n} (x_i^{1} = a_i) \text{ and } \phi_2 \triangleq \bigwedge_{1 \leq i \leq n} (x_i^{2} = a_i).
$$

**Proof.** The proof is similar to the case of independence (Proposition 13). 

### 6.2 Example: Conditional Independence

We consider a simple example often used to illustrate Bayesian networks models. Let $x, y, z$ and $w'$ be random variables, where $x, y$ and $z$ are sampled from distributions $\mu, \mu'$ and $\mu''$ respectively, and $w$ and $w'$ are defined by their respective assignments. Both $w$ and $w'$ depend on $y$, along with independent sources of randomness, respectively $x$ and $z$. While $w$ and $w'$ are not independent—they share dependence on $y$—if we condition on a particular value of $y$, then $w$ and $w'$ are independent.

![Figure 9: Conditional indep.](image)

The code of the corresponding program $s$ is given in Fig. 9. We want to show that $w$ and $w'$ are independent conditioned on $y = c$ for every $c$. Using our characterization based on self-composition, it amounts to proving the following (universally quantified) pRHL judgment:

$$
\vdash s^{(2)} \sim s^{(2)} : \text{EqMem}^{(2),(2)} \implies \phi^{(1)} \iff \psi^{(2)}
$$

where

$$
\phi \triangleq w^1 = a \land w'^1 = b \land y^1 = c \land y^2 = c
$$

$$
\psi \triangleq w^1 = a \land w'^2 = b \land y^1 = c \land y^2 = c.
$$

The proof proceeds by moving the samplings of $z^1$ and $z^2$ in both programs to the front of the program, and then swapping samplings in the left program (we can use the rule [SWAP] to reorder the instructions, as the sampling instructions for $z^1$ and $z^2$ operate on different variables). Then, we couple $z^1(1)$ to be equal to $z^2(2)$, and $z^2(1)$ to be equal to $z^1(2)$. We apply the identity coupling to all other random samplings.
7 Formalization

EasyCrypt [3, 4] is an interactive proof assistant that supports reasoning about (relational) properties of probabilistic programs, using the pRHL logic. We have applied EasyCrypt to the main examples of this paper. For uniformity, it suffices to establish the required pRHL judgment; in contrast, independence via self-composition requires to build the self-composed program, which we have done manually. The main challenges for the verification are:

1. Restructuring the code of the program to make the rules of the logic applicable; this is done by applying the equivalent of the [STRUCT] rules.
2. Discovering and establishing the correct proof invariants. The current version of EasyCrypt requires that invariants are produced by the users.
3. Building an appropriate coupling, primarily through applying the rule for random samplings with carefully chosen bijections.

Our examples are formalized in about 1,000 lines of proof script in EasyCrypt. The most complex example, and the one where the three challenges are most pronounced, is the random walk over a cycle. This example is formalized in about 500 lines of EasyCrypt code, out of which the statement, including the definition of the program, takes about 50 lines. The remaining 90% of the formalization covers the notions used in the proof and the proof itself.

8 Conclusion

We have proposed a new method based on probabilistic couplings for formally verifying uniformity and independence properties of probabilistic programs. Our method complements the existing range of techniques for probabilistic reasoning, and has many potential applications in program verification, security, and privacy.

9 Acknowledgments

We thank the anonymous reviewers for their detailed comments. This work was partially supported by NSF grants TC-1065060 and TWC-1513694, by the European Union’s H2020 Programme under grant agreement number ICT-644209, and a grant from the Simons Foundation (#360368 to Justin Hsu).

References


2Proofs are available at the following link: https://gitlab.com/easycrypt/indep


