Acta Informatica 39, 315–389 (2003)
Digital Object Identifier (DOI) 10.1007/s00236-003-0113-z

Reasoning about probabilistic sequential programs in a probabilistic logic

Mingsheng Ying[1,2⋆]

[1] State Key Laboratory of Intelligent Technology and Systems, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China (e-mail: yingmsh@tsinghua.edu.cn)

[2] Turku Center for Computer Science (TUCS), Software Construction Laboratory, Data City, Lemminkäisenkatu 14A, FIN-20520 Turku, Finland

Received: 16 April 2002 / 20 January 2003

Abstract. We introduce a notion of strong monotonicity of probabilistic predicate transformers. This notion enables us to establish a normal form theorem for monotone probabilistic predicate transformers. Three other healthiness conditions, namely, conjunctivity, disjunctivity and continuity for probabilistic predicate transformers are also examined, and they are linked to strong monotonicity. A notion of probabilistic refinement index is proposed, and it provides us with a continuous strength spectrum of refinement relations which may be used to describe more flexible refinement between probabilistic programs. A notion of probabilistic correctness is introduced too. We give a probabilistic weakest-precondition, choice and game semantics to the contract language, and present a probabilistic generalization of the winning strategy theorem.

Contents

⋆ This work was partly supported by the National Key Project for Fundamental Research of China (Grant No: 1998030905) and the National Foundation of Natural Sciences of China (Grant No: 60273003)

1 Introduction

Certain random phenomena are often involved in the analysis and design of complex software and hardware systems. This motivates us to develop some formal methods and mathematical tools for modelling and reasoning about programs containing probability information. Early in the 1980's, D. Kozen [20, 21] introduced probabilistic predicate transformers to give a weakest-precondition semantics of probabilistic programs. In his operational semantical model, a program is described as a mapping which associates a probability distribution over final states with each initial state, and the value of this distribution at a final state is explained as the probability that from the initial state an execution of the program will arrive at that final state. In 1989, C. Jones and G. Plotkin [19] constructed some probabilistic powerdomains as a denotational semantical model of probabilistic programs. Furthermore, these probabilistic powerdomains were used by C. Jones [18] to recast D. Kozen's probabilistic predicate transformers. The probabilistic programs studied by these authors are all deterministic in the sense that the probability distribution of their final states is completely predictable from the initial state although an exact final state cannot be determined by the initial state. Thus, angelic and demonic choices do not occur in their probabilistic programs. As is well known, the angelic and demonic nondeterminisms provide us with a great flexibility of programming, and they have been extensively investigated in the realm of standard non-probabilistic programming. The operational model of deterministic probabilistic programs was extended by J. He, K. Seidel and A. McIver [15] to accommodate demonic choices. They proposed two different models for Dijkstra's language of guarded commands [11] with an additional probabilistic choice operator, namely, the relational model and the lifted model. In their relational model, a probabilistic program is depicted as a mapping from the initial states to the convex and upward closed sets of probability distributions over the final states. Thus, a demonic nondeterminism appears at the stage of choosing a suitable probability distribution; and D. Kozen's operational model may be seen as a special case of J. He, K. Seidel and A. McIver's relational model provided we identify a probability distribution with its convex and upward closure. (It should be noted that convexity is not really appropriate for D. Kozen's model since his resulting sets are singletons.) In contrast, a nondeterministic probabilistic program is treated as a convex and upward closed set of deterministic probabilistic programs in the lifted model. Shortly after, C. Morgan, A. McIver and K. Seidel [29] established a partial Galois connection between D. Kozen's probabilistic predicate transformer semantics and J. He, K. Seidel and A. McIver's relational model of probabilistic programs. They further introduced a healthiness condition of sublinearity for probabilistic predicate transformers. It is interesting that sublinearity char-

acterizes exactly the class of probabilistic predicate transformers that may be generated by J. He, K. Seidel and A. McIver's relational model. This characterization is very beautiful, and it is based on an ingenious combination of a topological argument and several linear programming lemmas. Recently in [24], A. McIver and C. Morgan added angelic nondeterminism into their earlier theory, and thoroughly examined the hierarchy of the space of probabilistic predicate transformers in a way corresponding to R. -J. Back and J. von Wright's approach for non-probabilistic programming [3-4]. Their main results were also generalized into infinite state spaces by using some topological techniques.

The aim of the present paper is to develop further the theory of probabilistic sequential programming. The underlying logic of the previous works is obviously classical two-valued logic. Thus, the object language used to write programs is probabilistic in a sense, but the meta-language that we employ to talk about the properties of probabilistic programs is still a two-valued logical language, and it is out of harmony with the object language. Indeed, the expressive power of the meta-language is not strong enough, and sometimes such a meta-language is not competent to describe precisely probabilistic programs. The driving idea of the present paper is to employ a probabilistic logic instead as our logical tool for reasoning about probabilistic programs. This new logical device gives rise to a much subtler way of describing probabilistic programs and their semantical models, and the author believes that it will provide us with some new insights on probabilistic programming. In fact, in the setting of probabilistic logic we are able to present a new concept of probabilistic implication between probabilistic predicates. This concept is more flexible and accurate than the one given in [24, 25, 29]. A monotonicity of probabilistic predicate transformer was proposed by C. Morgan, A. McIver and K. Seidel [24, 25, 29] based on their probabilistic implication. A careful analysis tells us that this monotonicity is not strong enough to obtain a probabilistic generalization of R. -J. Back and J. von Wright's normal form theorem [3, 4, 45]. However, the notion of probabilistic implication newly introduced in this paper helps us to find a stronger monotonicity that is suited to establish a normal form theorem for probabilistic predicate transformers but missing in the previous literatures. At the same time, it also allows us to have two subtler notions of probabilistic refinement and correctness. More explicitly, using a probabilistic logic, we are able to define two measures that indicate the belief degrees or probabilities of refinement or correctness, respectively, for probabilistic programs. Thus, a refinement relation between probabilistic programs can be thought of as a probabilistic relation rather than an ordinary one, and two programs may satisfy a refinement relation with a non-zero belief probability less than 1. As well, a correctness notion of probabilistic programs may be seen as a

probabilistic predicate which gives a belief probability instead of saying a program is correct or not, absolutely, with respect to a specification.

1.1 Overview of the paper

This paper is organized as follows: in the remainder of this introduction we briefly recall some basic ideas and notions from probabilistic logic. We also make some conventions of notations. At the end of this introduction, we will expose more related works and compare them with the results given in the present paper.

In Sect. 2, we further give some preliminaries. In particular, we review the notions of probabilistic sequential program and probabilistic predicate transformer from [15, 20, 21, 24, 29]. Also, we recall several healthiness conditions for probabilistic predicate transformers introduced in [24, 29], namely, monotonicity, scaling, sub-additivity and $\ominus$-subdistribution.

In Sect. 3, we introduce the notion of probabilistic relation as a probabilistic predicate on a product state space and define three operations of probabilistic relations: inverse, composition, and reflexive and transitive closure. The difference from the case of ordinary relation is that the reflexive and transitive closure of a probabilistic relation is not necessary to be a probabilistic relation. This is mainly because of a boundness requirement in the definition of probabilistic predicate. For the case of finite state spaces, we find a sufficient and necessary condition under which the reflexive and transitive closure of a probabilistic relation is also a probabilistic relation. Moreover, we propose probabilistic angelic and demonic updates that are probabilistic predicate transformers induced from a probabilistic relation.

Both Sections 4 and 5 are devoted to studying some new healthiness conditions for probabilistic predicate transformers. In Sect. 4, we first define an implication strength index between probabilistic predicates. This enables us to introduce a new monotonicity, named strong monotonicity. Strong monotonicity is really stronger than the monotonicity given in [24, 29] which, for convenience, we call weak monotonicity in this paper. At the same time, strong monotonicity is implied by weak monotonicity plus the scaling property. We establish a normal form theorem for strongly monotone probabilistic predicate transformers which generalizes R. -J. Back and J. von Wright's normal form theorem for ordinary monotone predicate transformers [2-4, 45], and says that a probabilistic predicate transformer is strongly monotone if and only if it can be represented as the sequential composition of a probabilistic angelic update and a probabilistic demonic update. We may see that weak monotonicity is a reasonable probabilistic generalization of the monotonicity for ordinary predicate transformers if we use two-valued logic in the study of probabilistic programs. However, if the meta-logic is

replaced by a probabilistic logic, strong monotonicity will naturally come into our hands as a probabilistic generalization of ordinary monotonicity. It is illustrated that weak monotonicity is not strong enough to accommodate a normal form of the sequential composition of an angelic update and a demonic update. This is a witness of the advantage of probabilistic logic for reasoning about probabilistic programs.

Section 5 is concerned with probabilistic conjunctivity, disjunctivity and continuity. For each of the three healthiness conditions, we present a normal form theorem which expresses probabilistic predicate transformers satisfying it in terms of angelic or demonic update, assertion and assumption. Again, these normal form theorems generalize R. -J. Back and J. von Wright's corresponding results for ordinary predicate transformers [2-4, 45]. It is worth noting that in the normal forms of probabilistic conjunctivity, disjunctivity, continuity as well as monotonicity, we always have to appeal an extra condition, namely, the scaling property. This is very different from the non-probabilistic case. The reason is that the truth value of a non-probabilistic predicate is either 0 or 1, but the truth value of a probabilistic predicate ranges over the whole unit interval. In other words, a new dimension for depicting the truth values of predicates is added into the setting of probabilistic predicate transformers. The usage of the scaling property is exactly to control the additional dimension.

In Sect. 6, we introduce the notions of probabilistic refinement and probabilistic correctness. In the previous approaches to probabilistic programming, refinement was always treated as a sharp concept in the sense that a probabilistic program is refined by another or not, absolutely, and there is not a third possibility. The notion of correctness was considered in a similar way. This is because the adopted meta-logic there is two-valued. Such two-valued notions of refinement and correctness is often over-simplified for probabilistic programs. Since we use a probabilistic logic as our meta-logic, the probabilistic refinement proposed here is itself a probabilistic relation which, for each pair of probabilistic programs, gives the belief probability that the first program is refined by the second; and the probabilistic correctness is a probabilistic predicate that indicates the belief probability that a probabilistic program satisfies a specification. Thus, our description of and reasoning about various properties of probabilistic programs are much subtler. We show that probabilistic refinement is preserved by various program constructs. A reduction from probabilistic correctness of complex programs to that of simpler ones is presented; and a close connection between probabilistic refinement and probabilistic correctness is demonstrated.

In Sect. 7, we propose a probabilistic predicate transformer semantics and a probabilistic choice semantics of R. -J. Back and J. von Wright's contract language [4]. The probabilistic choice semantics may be seen as a

generalization of J. He, K. Seidel and A. K. McIver's relational semantical model. It is shown that probabilistic predicate transformer semantics and probabilistic choice semantics may be directly transferred to each other.

In Sect. 8, we give a game semantics to probabilistic contract language. The winning function of probabilistic game strategy is introduced so that R.-J. Back and J. von Wright's winning strategy theorem [4] can be generalized into probabilistic refinement calculus. It is observed that the essential part of the probabilistic winning strategy theorem is three distributivities of real numbers: the complete distributivity between infimum and supremum, and the infinite distributivities of multiplication over both infimum and supremum.

Section 9 is the concluding section in which we outline the main ideas of the present paper and point out some problems for the further studies.

Overall, the principal technical contribution of this paper is three-fold: (1) we establish the normal form theorem for some probabilistic healthiness condition of programs, including monotonicity, conjunctivity, disjunctivity and continuity; (2) we propose a "probabilized" and more flexible version of refinement and correctness for probabilistic programs; and (3) we introduce three semantics' for probabilistic programs, namely, precondition, choice and game semantics, and in particular, a probabilistic generalization of the winning strategy theorem in the game semantics is found.

1.2 Background and notations

For convenience of the reader, here we briefly review a probabilistic logical language, that is adopted in this paper as our meta-logical language, and its semantics. The history of probabilistic logics may be traced back to 1930's. The first approach of establishing a many-valued logic system with the conception in mathematical probability theory was made by H. Reichenbach [37] and Z. Zawirski [50], and their central idea is that of assigning likelihood values or probabilities to statements, which are supposed to satisfy the basic axioms for probability measure. For a thorough exposition of early works on probabilistic logics, we refer to R. Carnap [7]. Nowadays, many different systems of probabilistic logic have been proposed with various motivations and backgrounds [14, 32, 34]. A probabilistic logic is a continuous-valued logic and it has the unit interval as its set of truth values. A striking feature of many probabilistic logics is non-truth-functionality in the sense that the truth value of a compound statement is not determined by the truth values of its components [38, Chap. 2, Sect. 27]. The probabilistic logic that we adopt in this paper is, however, a truth-functional one. The truth valuation rules of this logic are given as follows:

$$\lceil \sim \varphi \rceil := 1 - \lceil \varphi \rceil,$$

$$\lceil \varphi \wedge \psi \rceil := \lceil \varphi \rceil \times \lceil \psi \rceil,$$
$$\lceil \varphi \vee \psi \rceil := \lceil \varphi \rceil + \lceil \psi \rceil - \lceil \varphi \rceil \times \lceil \psi \rceil,$$
$$\lceil \varphi \to \psi \rceil := \min(1, \frac{\lceil \psi \rceil}{\lceil \varphi \rceil}),$$
$$\lceil (\forall x)\varphi \rceil := (\sqcap \sigma : \Sigma \cdot \lceil \varphi[\sigma/x] \rceil),$$

and

$$\lceil (\exists x)\varphi \rceil := (\sqcup \sigma : \Sigma \cdot \lceil \varphi[\sigma/x] \rceil),$$

where Σ is the universe of discourse. We use $\lceil \varphi \rceil$ to express the truth value of logical formula φ. The symbols $\sim, \wedge, \vee$ and $\to$ stand for the connectives of negation, conjunction, disjunction and implication, respectively, and $(\forall x)$ and $(\exists x)$ are the universal and existential quantifiers, respectively. The formula $\varphi[\sigma/x]$ results from φ by substituting x with σ. We may note that these truth valuation rules for connectives are envisioned from some familiar formulas in probability theory. Remember that the probability of the complement of an event A is

$$p(A^C) = 1 - p(A).$$

This is very similar to the truth valuation formula of negation. Suppose that A and B are two independent events. Then the probabilities of their intersection and union are respectively

$$p(A \cap B) = p(A) \times p(B)$$

and

$$p(A \cup B) = p(A) + p(B) - p(A) \times p(B).$$

This motivates the truth valuation formulas of conjunction and disjunction; for example, the rule for disjunction is similar to the probability of sum of two events. It should be pointed out that the assumption made above of the independence of the events A and B is of course not valid in general. What we mean here is that the formulas for the probabilities of the intersection and union of two independent events A and B suggest us to choose the truth valuation rules for conjunction and disjunction presented above. If we consider a more general case in which A and B may not be independent, then the situation will be much more complicated, and it will lead to a non-truth-functional probabilistic logic. Certainly, such a logic is very useful in the analysis of probabilistic programs, and even more suitable for many cases. But we are not going to treat it carefully in the present paper, and we leave it as a topic for the further studies. The rule for implication is a counterpart of conditional probability. Indeed, the conditional probability of event A given B is

$$p(A \mid B) = p(A \cap B)/p(B),$$

and if A is a subset of B then

$$p(A \mid B) = p(A)/p(B).$$

The conditional probability formula suggests us to define the truth value of conditional $\phi \to \psi$ as $\lceil\psi\rceil/\lceil\phi\rceil$ for the case of $\lceil\phi\rceil \geq \lceil\psi\rceil$. It is reasonable to require that $\lceil\phi \to \psi\rceil = 1$ whenever $\lceil\phi\rceil \leq \lceil\psi\rceil$. The rules for quantifiers are common in many-valued logics. We assume that the unique designated truth value of the logic is 1. Thus, for a formula φ and a set of formula Λ, we say that φ is a (semantical) consequence of Λ, writing $\Lambda \models \varphi$, if $\lceil\varphi\rceil = 1$ whenever $\lceil\psi\rceil = 1$ for all $\psi \in \Lambda$. In particular, $\emptyset \models \varphi$ is abbreviated to $\models \varphi$, and in this case φ is said to be valid.

Following [24, 29], we use infix dot for function application, and use the syntax

$$(\sqcap x : X \mid \mathit{range} \cdot f.x) \text{ and } (\sqcup x : X \mid \mathit{range} \cdot f.x)$$

for the greatest lower bound and least upper bound, respectively, of the values of f when x ranges over the elements of x satisfying the condition range.

1.3 More related works

This paper is mainly concerned with semantical models of probabilistic sequential programs. As explained above, it is motivated by [15-25, 29], and based upon [24, 25, 29]. We also borrow some ideas from our previous works [47-49]. However, there are still a lot of other works about probabilistic programs.

D. Monniaux [30, 31] proposed a probabilistic extension of P. Cousot and R. Cousot's framework of abstract interpretation of programs [8]. The safety properties of probabilistic programs were analyzed in this setting [30]. D. Monniaux [31] also provided a scheme for proving automatically probabilistic termination of programs by using exponential bounds on the tail of the distribution.

In Sect. 3, we introduce angelic and demonic updates of probabilistic relations as two basic programming statements. A probabilistic relation is defined to be a probabilistic predicate, i.e., bounded real-valued (expectation) function on the product space of its domain and codomain. The inverse of a probabilistic (binary) relation is given by exchanging simply the two arguments, and the composition of two probabilistic relations is calculated by taking the supremum of the product of the probabilities in the component relations, left the middle argument ranging over their common state space. A different approach to the "probabilization" of relation is carried out by E. E. Doberkat [12, 13]. It is impossible here to go into any details of this

interesting and promising theory, but we would like to have at least a superficial perception of his ideas. Let X and Y be two Polish spaces, i.e., second countable and completely metrizable topological spaces. Both of them can be seen as measurable spaces where the measurable sets are taken to be the Borel sets generated by the equipped topology. We write $S(Y)$ for the set of all sub-probability measures on Y. Then $S(Y)$ will also be a Polish space after endowed with the weak topology. Now a stochastic (or probabilistic) relation is defined to be a Borel measurable mapping from X into $S(Y)$. The composition of stochastic relations is given as the Kleisli composition [22, Theorem 6.5.1]. The constructions of inverse and demonic product of stochastic relations were examined carefully too. Some similar ideas were also envisaged by S. Abramsky, A. Blute and P. Panangaden [1, 33]. They constructed a category of probabilistic relations and proved that it possesses a tensored *-category and thus enjoys most of the important properties of the category of usual (Boolean) relations. It should be noted that the notion of stochastic kernel in [1] is the same as that of our probabilistic relation bounded by 1, but with an additional condition of measurability.

In Sect. 8, we present a game semantics for probabilistic programs and establish a probabilistic generalization of R. -J. Back and J. von Wright's winning strategy theorem [4]. Indeed, the study of probabilistic games has a long history and can be traced back to as early as 1950's [40]. For a good survey on this topic, see [36]. One of the most recent papers on probabilistic games is [9] where L. de Alfaro and R. Majumdar presented a quantitative game $\mu-$calculus for two-player games played for an infinite number of rounds, with $\omega-$regular winning condition, and showed that the maximal winning probability can be expressed as the fixpoint formula in this calculus. We should point out that our treatment of probabilistic game semantics of programs is still at the very beginning and certainly needs a further elaboration. A thorough exploitation of the applications of probabilistic games to semantics of probabilistic programs is highly anticipated.

As said before, what concerns us in this paper is probabilistic sequential programming. Another line of research about probabilistic programs is related to concurrency, and a very active area along this line is probabilistic process algebras. There have been a considerable number of papers on this topic, but here we are going to mention only a few of them. K. Seidel [39] introduced a probabilistic variant of Hoare's CSP [17], and J. Baeten, J. A. Bergstra and S. A. Smolka [5] added probability information into J. A. Bergstra and J. -W. Klop's ACP [6]. Many different probabilistic extensions of R. Milner's CCS [27] have been proposed in the previous literature, and R. J. van Glabbeek, S. A. Smolka and B. Steffen [43] divided them into three categories : reactive models, generative models and stratified models. It was demonstrated by them that the three categories of probabilistic models

of processes plus the classical (non-probabilistic) ones form a hierarchy of abstraction: the reactive models is derivable from the generative models by abstracting from the relative probabilities of different actions; the generative models can be derived from the stratified ones by abstracting the level-wise structure of probabilistic branching; and the classical models is induced from all the probabilistic models by giving up probability information.

2 Probabilistic programs and predicate transformers

This section is a preliminary one, and here we review the notion of probabilistic sequential program and its predicate transformer semantics from the previous literatures [20, 21, 15, 24, 29].

Suppose that Σ is a countable state space. A (discrete sub-)probabilistic distribution over Σ is a function $F : \Sigma \to [0, 1]$ with

$$\sum_{\sigma:\Sigma} F.\sigma \leq 1.$$

The set of probability distributions over Σ is denoted by $\overline{\Sigma}$. An ordering $\sqsubseteq$ on $\overline{\Sigma}$ may be induced pointwise from the usual (arithmetic) ordering for numbers in the unit interval; namely, for any $F, F' : \overline{\Sigma}$, $F \sqsubseteq F'$ if and only if $F.\sigma \leq F'.\sigma$ for all $\sigma : \Sigma$ ([15], Definitions 2.1 and 2.3; [29], Definitions 2.1 and 2.2; [24], Definition 2.1). Let $p \in [0, 1]$. Then the probabilistic choice operator ${}_p\oplus : \overline{\Sigma} \times \overline{\Sigma} \to \overline{\Sigma}$ is a binary operation on $\overline{\Sigma}$ and is defined as follows: for any $F, F' : \overline{\Sigma}$ and $\sigma : \Sigma$,

$$(F_p \oplus F').s := p \times F.s + (1 - p) \times F'.s.$$

A subset U of $\overline{\Sigma}$ is said to be upward closed if $F \in U$ and $F \sqsubseteq F'$ imply $F' \in U$. If for all $p \in [0, 1]$ and $F, F' \in U$ we always have $F_p \oplus F' \in U$, then U is called convex. Moreover, a subset U of $\overline{\Sigma}$ is also a subset of the Euclidean space $\mathbf{R}^{|\Sigma|}$ of dimension $\mid \Sigma \mid$, where $\mathbf{R}$ stands for the set of real numbers, and $\mid \Sigma \mid$ is the cardinality of Σ. We call U Cauchy-closed when U is a closed subset of $\mathbf{R}^{|\Sigma|}$ according to the usual (Euclidean) topology. Let $U \subseteq \overline{\Sigma}$. The upward closure $\uparrow U$ of U is defined to be the smallest upward closed subset of $\overline{\Sigma}$ containing U, and the convex-closure $cc.U$ is the smallest convex subset of $\overline{\Sigma}$ containing U. We write $\mathbf{C}\Sigma$ for the set of non-empty, upward closed, convex and Cauchy-closed subsets of $\overline{\Sigma}$. A probabilistic demonic program from state space Σ to state space Γ is a mapping P from Σ into $\mathbf{C}\Gamma$. The space of probabilistic demonic programs from Σ to Γ is written as

$$\mathbf{P}(\Sigma, \Gamma) := \Sigma \to \mathbf{C}\Gamma.$$

A probabilistic program $P : \mathbf{P}(\Sigma, \Gamma)$ is said to be deterministic if for any state $\sigma : \Sigma$, $P.\sigma$ is the upward closure of a single distribution F_σ on Γ, i.e.,

$$P.\sigma = \{F : \overline{\Gamma} \mid F_\sigma \sqsubseteq F\}$$

The refinement ordering $\sqsubseteq$ on probabilistic demonic programs is induced pointwise by the inclusion relation on $\mathbf{C}\Gamma$, and it is defined as follows: for any $P, P' : \mathbf{P}(\Sigma, \Gamma)$,

$$P \sqsubseteq P' := (\forall \sigma : \Sigma \cdot P.\sigma \supseteq P'.\sigma).$$

([15], page 176; [29], Definition 5.4; [24], Definition 2.4).

We now further recall the notion of probabilistic predicate and probabilistic implication relation between probabilistic predicates. We denote the set of non-negative reals by $\mathbf{R}_{\geq}$. Recall that a predicate in the classical refinement calculus is a Boolean-valued function on the state space. Nevertheless, a probabilistic predicate on the state space Σ is defined to be a bounded expectation on Σ, namely, a function α of type $\Sigma \to \mathbf{R}_{\geq}$ such that there is $M \in \mathbf{R}_{\geq}$ with $\alpha.\sigma \leq M$ for all $\sigma : \Sigma$ ([29], Definition 6.1.1; [24], pages 333-334). The reason that the values of a probabilistic predicate are allowed to exceed 1 may be seen from the definition below of weakest precondition of a probabilistic program where the expected value of a real-valued function α over a probability distribution appears, and it is not necessarily less than or equal to 1. In particular, if a is a non-negative real and σ_0 is a state in Σ, then the constant function $\underline{a}$, $\underline{a}.\sigma = a$ for every $\sigma : \Sigma$, and the singleton $\overline{\sigma_0}$,

$$\overline{\sigma_0}.\sigma = \begin{cases} 1 \text{ if } \sigma = \sigma_0, \\ 0 \text{ otherwise} \end{cases}$$

are both probabilistic predicates. We write $\mathbf{P}\Sigma$ for the set of probabilistic predicates. There is a natural partial ordering $\equiv>$ on $\mathbf{P}\Sigma$, called probabilistic implication. It is induced pointwise from the usual (arithmetic) ordering on the non-negative reals $\mathbf{R}_{\geq}$, and defined as follows: for any $\alpha, \beta : \mathbf{P}\Sigma$,

$$\alpha \equiv> \beta := (\forall \sigma : \Sigma \cdot \alpha.\sigma \leq \beta.\sigma).$$

Intuitively, $\equiv>$ means "everywhere no more than". We sometimes write $\alpha <\equiv \beta$ for $\beta \equiv> \alpha$. Thus the identity relation on $\mathbf{P}\Sigma$ may be expressed in terms of $\equiv>$:

$$\alpha \equiv \beta := (\alpha \equiv> \beta \wedge \alpha <\equiv \beta).$$

It is easy to see that $<\equiv$ means "everywhere no less than", and $\equiv$ means "everywhere equal to" ([29], Definition 6.1.1; [24], pages 334).

The algebraic structure of the probabilistic predicate space $(\mathbf{P}\Sigma, \equiv>)$ is simple, and it is a distributive lattice. Its bottom element if $false$, where for each $\sigma : \Sigma$, $false.\sigma = 0$. We write $\sqcap$ and $\sqcup$ for the greatest lower bound and the least upper bound, respectively, in $(\mathbf{P}\Sigma, \equiv>)$. Then $\mathbf{P}\Sigma$ is $\sqcap-$complete, but not $\sqcup-$ complete because the least upper bound of infinite bounded expectations may be no longer bounded. For any family $\{\alpha_i \mid i \in I\}$ of probabilistic predicates over Σ, and for all $\sigma : \Sigma$,

$$(\sqcap i \in I \cdot \alpha_i).\sigma = (\sqcap i \in I \cdot \alpha_i.\sigma),$$

$$(\sqcup i \in I \cdot \alpha_i).\sigma = (\sqcup i \in I \cdot \alpha_i.\sigma)$$

if $(\sqcup i \in I \cdot \alpha_i)$ exists. Since $\mathbf{P}\Sigma$ has no top element, it is impossible to define a complement operation so that $\mathbf{P}\Sigma$ becomes a Boolean algebra. To clarify further the difference between the algebraic properties of the probabilistic predicate space and the usual predicate space, we recall the notion of atom. Let $(L, \sqsubseteq)$ be a lattice with the bottom element $\bot$. Then $a \in L - \{\bot\}$ is called an atom if for each $b \in L$, $b \sqsubseteq a$ implies $b = \bot$ or $b = a$. A lattice L is said to be atomic if for any $x \in L$, it holds that

$$x = \sqcup\{a \in L : a \sqsubseteq x \text{ and } a \text{ is an atom}\},$$

where $\sqcup$ stands for the least upper bound in L. It is easy to see that $\mathbf{P}\Sigma$ is atomless; that is, $\mathbf{P}\Sigma$ does not have any atom. However, it was shown that the usual predicate space is an atomic Boolean algebra ([4], Theorem 2.3).

We can also define the arithmetic operations on $\mathbf{P}\Sigma$. Let $\alpha, \beta : \mathbf{P}\Sigma$. Then the sum $\alpha + \beta$, arithmetic subtraction $\alpha \ominus \beta$, and product $\alpha \times \beta$ are all in $\mathbf{P}\Sigma$ and for each $\sigma : \Sigma$,

$$(\alpha + \beta).\sigma := \alpha.\sigma + \beta.\sigma,$$

$$(\alpha \ominus \beta).\sigma := \max(0, \alpha.\sigma - \beta.\sigma),$$

$$(\alpha \times \beta).\sigma := \alpha.\sigma \times \beta.\sigma.$$

In particular, we usually write $\underline{a} \times \alpha$ in the form of scalar product $a \times \alpha$. It is obvious that the operations defined above on probabilistic predicates are the pointwise extensions of the corresponding operations on real numbers.

Definition 1. *([29], Definition 6.1.1; [24], Definition 2.5) Let Σ and Γ be two state spaces.*

(1) A probabilistic predicate transformer from Σ to Γ is a mapping from $\mathbf{P}\Gamma$ into $\mathbf{P}\Sigma$. The space of probabilistic predicate transformers is denoted by $\Sigma \mapsto \Gamma$, that is,

$$\Sigma \mapsto \Gamma := \mathbf{P}\Gamma \to \mathbf{P}\Sigma.$$

(2) A probabilistic predicate transformer $t : \Sigma \mapsto \Gamma$ is said to be monotone if for any $\alpha, \alpha' : \mathbf{P}\Gamma$,

$$\alpha \equiv> \alpha' \text{ implies } t.\alpha \equiv> t.\alpha'.$$

We write $\Sigma \mapsto_m \Gamma$ for the space of monotone probabilistic predicate transformers.
(3) The refinement ordering $\sqsubseteq$ on probabilistic predicate transformers is the pointwise extension of probabilistic implication $\equiv>$ on probabilistic predicates, and it is defined by

$$t \sqsubseteq t' := (\forall \alpha : \mathbf{P}\Gamma \cdot t.\alpha \equiv> t'.\alpha)$$

for all $t, t' : \Sigma \mapsto \Gamma$.

It is clear that $(\Sigma \mapsto \Gamma, \equiv>)$ is a distributive lattice and it is meet-complete but not join-complete. $\Sigma \mapsto_m \Gamma$ is a sublattice of $\Sigma \mapsto \Gamma$. All operations on probabilistic predicates may be pointwise extended to probabilistic predicate transformers:

$$\begin{aligned}
(\sqcap i \in I \cdot t_i).\alpha &:= (\sqcup i \in I \cdot t_i.\alpha), \\
(\sqcup i \in I \cdot t_i).\alpha &:= (\sqcup i \in I \cdot t_i.\alpha), \\
(t + t').\alpha &:= t.\alpha + t'.\alpha, \\
(t \ominus t').\alpha &:= t.\alpha \ominus t'.\alpha, \\
(t \times t').\alpha &:= t.\alpha \times t'.\alpha
\end{aligned}$$

for all $t, t', t_i \ (i \in I) : \Sigma \mapsto \Gamma$ and $\alpha : \mathbf{P}\Gamma$. Another important operation of probabilistic predicate transformers is sequential composition which has no counterpart in operations of probabilistic predicates. Let $t : \Sigma \mapsto \Gamma$ and $t' : \Gamma \mapsto \Delta$. Then the sequential composition $t; t' : \Sigma \mapsto \Delta$ of t and t' is defined by $(t; t').\alpha = t.(t'.\alpha)$ for all $\alpha : \mathbf{P}\Delta$. It is worth noting that all the properties, relations and operation introduced above for probabilistic predicate transformers are defined in a pointwise way.

Probabilistic programs and predicate transformers are closely related to each other. Let $P : \mathbf{P}(\Sigma, \Gamma)$ be a probabilistic demonic program. Then the probabilistic predicate transformer $wp.P$ of P is defined to be an element in $\Sigma \mapsto \Gamma$ and for all $\alpha : \mathbf{P}\Gamma$ and $\sigma : \Sigma$,

$$wp.P.\alpha.\sigma = \left(\sqcap F : P.\sigma \cdot \int_F \alpha\right),$$

where $\int_F \alpha$ is the expected value of the real-valued function α over the probabilistic distribution F on Γ, that is,

$$\int_F \alpha = \sum_{\gamma : \Gamma} F.\gamma \times \alpha.\gamma.$$

Conversely, for any predicate transformer $t : \Sigma \mapsto \Gamma$, the least probabilistic program $rp.t : \mathbf{P}(\Sigma, \Gamma)$ induced by t is defined by

$$rp.t.\sigma := \left\{ F : \overline{\Gamma} \mid \left(\forall \alpha : \mathbf{P}\Gamma \cdot t.\alpha.\sigma \leq \int_F \alpha \right) \right\},$$

for every $\sigma : \Sigma$. Here, the word "least" means that for any $P : \mathbf{P}(\Sigma, \Gamma)$ with $t \sqsubseteq wp.P$, we have $rp.t \sqsubseteq P$. Note that the right-hand side of the above defining equation might be an empty set, and in this case $rp.t.\sigma$ is undefined.

It was shown by C. Morgan, A. McIver and K. Seidel [24, 29] that wp and rp form a partial Galois connection, that is, $rp.(wp.P) = P$ for each $P : \mathbf{P}(\Sigma, \Gamma)$ and $t \sqsubseteq wp.(rp.t)$ whenever $t : \Sigma \mapsto \Gamma$ and $rp.t$ is defined. They also introduced three healthiness conditions for probabilistic transformers $t : \Sigma \mapsto \Gamma$. These properties characterize exactly the wp-images of $\mathbf{P}(\Sigma, \Gamma)$ ([29], Theorem 8.7; [24], Theorem 2.9), and they are defined as follows: for all $a : \mathbf{R}_{\geq}$ and $\alpha : \mathbf{P}\Gamma$,
(1) Scaling: $t.(a \times \alpha) \equiv a \times t.\alpha$.
(2) Sub-additivity: $t.(\alpha + \alpha') <\equiv t.\alpha + t.\alpha'$.
(3) $\ominus$-subdistribution: $t.(\alpha \ominus \underline{a}) <\equiv t.\alpha \ominus \underline{a}$.

The above three properties are collectively referred to as sublinearity. Sub-additivity may be strengthened by

(2') Additivity: $t.(\alpha + \alpha') \equiv t.\alpha + t.\alpha'$ for all $\alpha, \alpha' : \mathbf{P}\Gamma$.

Additivity, scaling and $\ominus$-subdistribution together are named as linearity. (In Sect. 5, it will be seen that additivity implies the scaling property.) It was proved that linearity properly describes the $wp-$images of deterministic probabilistic programs ([24], Theorem 3.5).

3 Probabilistic relational updates

A Boolean relation R from the state space Σ to Γ is usually defined to be a mapping from Σ into the power set of Γ, which is isomorphic to the space of Boolean predicates on Γ (see [4], page 151). On the other hand, a Boolean relation from Σ to Γ can also be seen as a Boolean predicate on the Cartesian product $\Sigma \times \Gamma$. This observation suggests us to give a definition of probabilistic relation.

Definition 2. *Let Σ and Γ be two state spaces. A probabilistic relation R from Σ to Γ is a probabilistic predicate on the product type $\Sigma \times \Gamma$. We write $\Sigma \leftrightarrow \Gamma$ for the space of probabilistic relations from Σ to Γ, that is,*

$$\Sigma \leftrightarrow \Gamma := \mathbf{P}(\Sigma \times \Gamma).$$

A question naturally arises from the above definition: why we do not define a probabilistic relation from Σ to Γ to be a function from Σ into $\mathbf{P}\Gamma$ in the way similar to that of defining a Boolean relation? The reason is that a definition given in such a way would need a boundedness condition much more complex than that we used above. To explain our design decision more explicitly, let us see what will happen if we adopt a definition of probabilistic relations similar to that of Boolean relations. Suppose that R is a function from Σ into $\mathbf{P}\Gamma$. For every $\gamma : \Gamma$ we define the projection $R_\Sigma.\gamma : \Sigma \to R_\geq$ of R on Σ at γ as follows: for every $\sigma : \Sigma$,

$$(R_\Sigma.\gamma).\sigma := R.\sigma.\gamma.$$

It is easy to see that $R_\Sigma.\gamma$ is not necessarily bounded, that is, we may have $R_\Sigma.\gamma \notin \mathbf{P}\Sigma$. This is not reasonable because it breaks the symmetry between the two state variables σ and γ in $R.\sigma.\gamma$. Moreover, it will be seen that this non-symmetry causes a difficulty for defining the inverse of probabilistic relation: the inverse of a probabilistic relation may not be a probabilistic relation if we define a probabilistic relation as a mapping from Σ into $\mathbf{P}\Gamma$. A similar difficulty appears for the composition of probabilistic relations. One may argue that a slight modification will give us a reasonable definition of probabilistic relations provided we require further the boundedness of $R_\Sigma.\gamma$ for all $\gamma : \Gamma$. However, this is still not equivalent to our original definition of probabilistic relations as probabilistic predicates on $\Sigma \times \Gamma$. For example, let $\Sigma = \Gamma =$ the non-negative integers, and let $R.\sigma.\gamma = \min(\sigma, \gamma)$ for any $\sigma : \Sigma$ and $\gamma : \Gamma$. Then both $R.\sigma$ and $R_\Sigma.\gamma$ are bounded for all σ and γ, but R is not a probabilistic predicate on $\Sigma \times \Gamma$ because for any non-negative real M,

$$R.([M]+1).([M]+1) = [M]+1 > M,$$

where $[M]$ stands for the biggest integer that is not greater than M. More importantly, the boundedness of both $R.\sigma$ and $R_\Sigma.\gamma$ need not to guarantee that a composition of two probabilistic relations is well defined. This will become even clearer when we give an example after Lemma 1 below.

It is well-known that Boolean relations from Σ to Γ form a complete, Boolean, and atomic lattice. The algebraic structure of the space of probabilistic relations is quite different. It is easy to see that the algebraic structure of $(\Sigma \leftrightarrow \Gamma, \equiv>)$ is the same as that of the probabilistic predicate space. Indeed, $\Sigma \leftrightarrow \Gamma$ is exactly the set of probabilistic predicates over the product type $\Sigma \times \Gamma$. Since probabilistic relations are probabilistic predicates on a certain product type, the notion of probabilistic implication for probabilistic predicates is directly applied to them. $\Sigma \leftrightarrow \Gamma$ has the bottom:

$$\mathit{False}.\sigma.\gamma := 0$$

for every $\sigma : \Sigma$ and $\gamma : \Gamma$. The greatest lower bound and the least upper bound in $(\Sigma \leftrightarrow \Gamma, \equiv>)$ are also denoted by $\sqcap$ and $\sqcup$, respectively.

Each probabilistic predicate $\alpha : \mathbf{P}\Sigma$ induces a diagonal probabilistic relation $\mid \alpha \mid : \Sigma \leftrightarrow \Sigma$ as follows: for all $\sigma, \gamma : \Sigma$,

$$\mid \alpha \mid .\sigma.\gamma := \begin{cases} \alpha.\sigma \text{ if } \sigma = \gamma, \\ 0 \text{ otherwise.} \end{cases}$$

Each Boolean relation R from Σ to Γ can be seen as a probabilistic relation if we identify it with its characteristic function. In particular, the identity relation is a probabilistic relation. All operations of probabilistic predicates can be directly used to probabilistic relations. In addition, we may define two new operations on probabilistic relations.

Definition 3. *Let $P : \Sigma \leftrightarrow \Gamma$ and $Q : \Gamma \leftrightarrow \Delta$.*
(1) The inverse $P^{-1} : \Gamma \times \Sigma \to \mathbf{R}_{\geq}$ is given by

$$P^{-1}.\gamma.\sigma := P.\sigma.\gamma$$

for all $\gamma : \Gamma$ and $\sigma : \Sigma$.
(2) The composition $P \circ Q : \Sigma \times \Delta \to \mathbf{R}_{\geq}$ is defined by

$$(P \circ Q).\sigma.\delta := (\sqcup\gamma : \Gamma \cdot P.\sigma.\gamma \times Q.\gamma.\delta)$$

for all $\sigma : \Sigma$ and $\delta : \Delta$.

Recall that the composition of Boolean relations is defined by the following equation:

$$(P \circ Q).\sigma.\delta := (\exists\gamma : \Gamma \cdot P.\sigma.\gamma \wedge Q.\gamma.\delta)$$

(see [4], page 153), and note that in probabilistic logic the existential quantifier is interpreted as supremum, and conjunction as product of truth values. We can see that the defining equation of the composition of probabilistic relations is a probabilistic interpretation of that for Boolean relations. It should be pointed out that Definition 3(2) does not exactly fall into the framework of probabilistic logic because $P.\sigma.\gamma$ and $Q.\gamma.\delta$ are allowed to exceed 1 but the truth values in probabilistic logics are required to be in the unit interval. So, it is merely a formula in an analogue of probabilistic logic. This remark also applies to the probabilistic logical interpretations of some other definitions below. The following lemma explains further the reasonableness of Definition 3.

Lemma 1. *If $P : \Sigma \leftrightarrow \Gamma$ and $Q : \Gamma \leftrightarrow \Delta$, then $P^{-1} : \Gamma \leftrightarrow \Sigma$ and $P \circ Q : \Sigma \leftrightarrow \Delta$.*

Proof. We only consider the case of $P \circ Q$. It suffices to show that $P \circ Q$ is bounded. The boundedness of P and Q states that there are $M, N \geq 0$

with $P.\sigma.\gamma \leq M$ for all $\sigma : \Sigma$ and $\gamma : \Gamma$, and $Q.\gamma.\delta \leq N$ for all $\gamma : \Gamma$ and $\delta : \Delta$. Then for any $\sigma : \Sigma$ and $\delta : \Delta$, it follows that

$$\begin{aligned}(P \circ Q).\sigma.\delta &= (\sqcup\gamma : \Gamma \cdot P.\sigma.\gamma \times Q.\gamma.\delta) \\ &\leq (\sqcup\gamma : \Gamma \cdot M \times Q.\gamma.\delta) \\ &\leq M \times N,\end{aligned}$$

and $P \circ Q$ is really bounded.#

It was pointed out that the boundedness of the composition of probabilistic relations may be violated if we define a probabilistic relation from Σ to Γ as a mapping from Σ into $\mathbf{P}\Gamma$. Here we present an example to illustrate explicitly this fact. Let $\Sigma = \Gamma = \Delta =$ the non-negative integers, and let $P.\sigma.\gamma = 1$ and $Q.\gamma.\delta = \min(\gamma, \delta)$ for any $\sigma : \Sigma$, $\gamma : \Gamma$ and $\delta : \Delta$. Then $(P \circ Q).\sigma.\delta = \delta$, and $(P \circ Q).\sigma$ is not bounded because δ may range over all non-negative integers.

Some basic properties of composition are collected in the next proposition, and their proofs are easy and so omitted.

Proposition 2. *Let $R, P, P_i\ (i \in I) : \Sigma \leftrightarrow \Gamma$ and $Q, Q_i\ (i \in I) : \Gamma \leftrightarrow \Delta$. Then*
(1) $Id \circ R = R \circ Id = R$, where Id is the identity relation on the respective state spaces.
(2) $False \circ R = False$, $R \circ False = False$, where $False$ is the empty relation on the respective state spaces.
(3) $P \circ (\sqcup i \in I \cdot Q_i) = (\sqcup i \in I \cdot P \circ Q_i)$ if $(\sqcup i \in I \cdot Q_i)$ exists.
(4) $(\sqcup i \in I \cdot P_i) \circ Q = (\sqcup i \in I \cdot P_i \circ Q)$ if $(\sqcup i \in I \cdot P_i)$ exists.#

The reflexive and transitive closure of a Boolean relation may help us to analyze iterated constructs of non-probabilistic programs. Similarly, we can introduce the notion of reflexive and transitive closure of a probabilistic relation.

Definition 4. *Let Σ be a state space and $R : \Sigma \leftrightarrow \Sigma$. Then the reflexive and transitive closure $R^* : \Sigma \times \Sigma \to \mathbf{R}_{\geq} \cup \{+\infty\}$ of R is defined by*

$$R^* := (\sqcup n : \omega \cdot R^n),$$

where ω is the set of non-negative integers, and R^n is defined by induction on n :

$$\begin{cases} R^0 := Id_{\Sigma}, \\ R^{n+1} := R \circ R^n,\ n = 0, 1, 2, ... \end{cases}$$

The treatment of reflexive and transitive closure of a probabilistic relation is much more difficult than the treatment of Boolean relations. In particular,

the reflexive and transitive closure of a probabilistic relation may not even be a probabilistic relation. The following theorem gives a necessary and sufficient condition under which R^* is a probabilistic relation for the case of finite state spaces.

Theorem 3. *Let Σ be a finite state space and $R : \Sigma \leftrightarrow \Sigma$. Then $R^* \notin \Sigma \leftrightarrow \Sigma$ if and only if there are non-negative integer n and $\sigma_0, \sigma_1, ..., \sigma_n : \Sigma$ such that*

$$(\Pi_{i=0}^{n} R.\sigma_i.\sigma_{i+1}) \times R.\sigma_n.\sigma_0 > 1.$$

Proof. ($\Leftarrow$) If

$$(\Pi_{i=0}^{n} R.\sigma_i.\sigma_{i+1}) \times R.\sigma_n.\sigma_0 > 1,$$

then for any $k \in \omega$, we have

$$R^*.\sigma_0.\sigma_0 = (\sqcup m : \omega.\gamma_1, ..., \gamma_{m-1} : \Sigma \cdot R.\sigma_0.\gamma_1 \times ... \times R.\gamma_i.\gamma_{i+1} \times ... \times R.\gamma_{m-1}.\sigma_0) \geq [(\Pi_{i=0}^{n} R.\sigma_i.\sigma_{i+1}) \times R.\sigma_n.\sigma_0]^k.$$

Thus, $R^*.\sigma_0.\sigma_0 = +\infty$ and $R^* \notin \Sigma \leftrightarrow \Sigma$.

($\Rightarrow$) Suppose that $R^* \notin \Sigma \leftrightarrow \Sigma$, and for all $n : \omega$ and $\sigma_0, \sigma_1, ..., \sigma_n : \Sigma$,

$$(\Pi_{i=0}^{n} R.\sigma_i.\sigma_{i+1}) \times R.\sigma_n.\sigma_0 \leq 1.$$

We aim at deriving a contradiction. Since $R^* \notin \Sigma \leftrightarrow \Sigma$ and Σ is finite, there are $\sigma, \gamma : \Sigma$ such that $R^*.\sigma.\gamma = +\infty$. Furthermore, from the definition of R^* we know that for every $N : \omega$, there are $\delta_{N1}, ..., \delta_{Nl_N} : \Sigma$ with

$$R.\sigma.\delta_{N1} \times ... \times R.\delta_{Nk}.\delta_{N(k+1)} \times ... \times R.\delta_{Nl_N}.\gamma \geq N.$$

Note that we can always take $l_N \leq \mid \Sigma \mid$. In fact, if $l_N > \mid \Sigma \mid$, then two of elements $\sigma, \delta_{N1}, ..., \delta_{Nl_N}, \gamma$ should be identical. Assume that $\delta_{Ni} = \delta_{Nj}$ $(0 \leq i < j \leq l_N + 1)$, where we use δ_{N0} and $\delta_{N(l_N+1)}$ to denote σ and γ, respectively. Then

$$R.\delta_{Ni}.\delta_{N(j+1)} = R.\delta_{Nj}.\delta_{N(j+1)},$$

and from the assumption we have

$$\Pi_{k=i}^{j-1} R.\delta_{Nk}.\delta_{N(k+1)} \leq 1.$$

This yields

$$R.\sigma.\delta_{N1} \times ... \times R.\delta_{N(i-1)}.\delta_{Ni} \times R.\delta_{Ni}.\delta_{N(j+1)} \times ... \times R.\delta_{Nl_N}.\gamma \geq R.\sigma.\delta_{N1} \times ... \times R.\delta_{Nk}.\delta_{N(k+1)} \times ... \times R.\delta_{Nl_N}.\gamma \geq N.$$

We repeat this process and finally reduce l_N to some integer not greater than $\mid \Sigma \mid$. On the other hand, we can find some $M \in \mathbf{R}_{\geq}$ such that $R.\delta.\delta' \leq M$ for all $\delta, \delta' : \Sigma$ because R is in $\Sigma \leftrightarrow \Sigma$. Then

$$N \leq R.\sigma.\delta_{N1} \times ... \times R.\delta_{N(i-1)}.\delta_{Ni} \times R.\delta_{Ni}.\delta_{N(j+1)} \times ... \times R.\delta_{Nl_N}.\gamma \leq M^{|\Sigma|+1}.$$

This contradicts that N can range over all non-negative integers.#

A simple corollary is concerned with symmetric probabilistic relations.

Corollary 4. *If R is symmetric, i.e., $R = R^{-1}$, then $R^* \in \Sigma \leftrightarrow \Sigma$ if and only if $R.\sigma.\gamma \leq 1$ for all $\sigma, \gamma : \Sigma$.*

Proof. ($\Leftarrow$) Obvious.

($\Rightarrow$) From the above theorem and symmetry of R we know that

$$(R.\sigma.\gamma)^2 = R.\sigma.\gamma \times R.\gamma.\sigma \leq 1$$

and therefore $R.\sigma.\gamma \leq 1$.#

From its proof we can see that the "if" part of Theorem 3 is also valid for infinite state spaces. However, the "only-if" part does not hold for infinite state spaces. Indeed, if there are infinitely many elements $\sigma_0, \sigma_1, \sigma_2, ...$ in Σ and a real $r > 1$ such that $R.\sigma_i.\sigma_{i+1} > r$ for all $i = 0, 1, 2, ...$, we have $R^* \notin \Sigma \leftrightarrow \Sigma$. The next proposition shows that the value of a reflexive and transitive closure at the diagonal is either infinite or not greater than 1.

Proposition 5. *Let Σ be a state space and $R : \Sigma \leftrightarrow \Sigma$. Then for any $\sigma : \Sigma$, we have $R^*.\sigma.\sigma \in [0, 1] \cup \{+\infty\}$.*

Proof. It suffices to note that

$$\begin{aligned}(R^*.\sigma.\sigma)^2 &= (\sqcup n : \omega.\sigma_1, ..., \sigma_{n-1} : \Sigma \cdot R.\sigma.\sigma_1 \times ... \times R.\sigma_{n-1}.\sigma)^2 \\ &= (\sqcup n, n' : \omega.\sigma_1, ..., \sigma_{n-1}, \sigma'_1, ..., \sigma'_{n'-1} : \Sigma.R.\sigma.\sigma_1 \\ &\times ... \times R.\sigma_{n-1}.\sigma \times R.\sigma.\sigma'_1 \times ... \times R.\sigma'_{n'-1}.\sigma) \\ &\leq R^*.\sigma.\sigma.\#\end{aligned}$$

The above results show that many probabilistic relations have no reflexive and transitive closure applicable in the construction of programs. This will bring an essential difficulty to us when dealing with recursion of probabilistic programs. We will further expose this point in Sect. 9.

The domain and range of a probabilistic relation will be needed in the study of correctness of probabilistic programs, so here we give their definitions.

Definition 5. *Let Σ and Γ be state spaces and $R : \Sigma \leftrightarrow \Gamma$. Then the domain $dom.R : \mathbf{P}\Sigma$ and the range $ran.R : \mathbf{P}\Gamma$ of R are defined respectively as follows: for any $\sigma : \Sigma$ and $\gamma : \Gamma$,*

$$dom.R.\sigma = (\sqcup \gamma' : \Gamma \cdot R.\sigma.\gamma'),$$

and

$$ran.R.\gamma = (\sqcup \sigma' : \Sigma \cdot R.\sigma'.\gamma)$$

We now are ready to introduce the key notions of angelic and demonic updates in the setting of probabilistic programming. To motivate our definition of probabilistic updates, we recall the corresponding notion for Boolean relations. Let R be a Boolean relation from Σ to Γ. The angelic update $\{R\}$ in initial state σ establishes postcondition q if there is a final state γ satisfying q with $R.\sigma.\gamma$, and the angel may choose it. On the other hand, the demonic update $[R]$ in initial state σ establishes postcondition q if we have $\gamma \in q$ for all final states γ with $R.\sigma.\gamma$ that the demon may choose. Formally, this can be written as follows:

$$\{R\}.q.\sigma := (\exists \gamma : \Gamma \cdot R.\sigma.\gamma \wedge q.\gamma),$$

$$[R].q.\sigma := (\forall \gamma : \Gamma \cdot R.\sigma.\gamma \Rightarrow q.\gamma).$$

By translating the above two logical formulae into probabilistic logic, we obtain the following:

Definition 6. *Let Σ and Γ be two state spaces, and let $R : \Sigma \leftrightarrow \Gamma$.*
(1) The angelic update $\{R\}$ is defined to be a probabilistic predicate transformer in $\Sigma \mapsto \Gamma$, and it is given by

$$\{R\}.\alpha.\sigma := (\sqcup \gamma : \Gamma \cdot R.\sigma.\gamma \times \alpha.\gamma)$$

for all $\alpha : \mathbf{P}\Gamma$ and $\sigma : \Sigma$.
(2) The demonic update $[R] : \Sigma \mapsto \Gamma$ is defined by

$$[R].\alpha.\sigma := \left(\sqcap \gamma : \Gamma \cdot \min\left(1, \frac{\alpha.\gamma}{R.\sigma.\gamma}\right)\right)$$

for all $\alpha : \mathbf{P}\Gamma$ and $\sigma : \Sigma$.

It may be seen that the defining equations of the probabilistic updates $\{R\}$ and $[R]$ come directly from applying the truth valuation rules of probabilistic logic to the defining formulas of the Boolean updates. In particular, the upper bound operation $\min(1, \cdot)$ in the defining equation of $[R]$ is given

by the rule for implication and its aim is to make the truth value not greater than 1. Indeed, this operation can be left out; that is,

$$[R].\alpha.\sigma := \min\left(1, \left(\sqcap\gamma : \Gamma \cdot \frac{\alpha.\gamma}{R.\sigma.\gamma}\right)\right).$$

In addition, if we use the notion of implication strength introduced in Definition 7 below, it can also be rewritten as follows:

$$[R].\alpha.\sigma = \lceil R_\Gamma.\sigma \equiv> \alpha \rceil,$$

where $R_\Gamma.\sigma$ is the projection of R on Γ at σ, namely, for every $\gamma \in \Gamma$,

$$(R_\Gamma.\sigma).\gamma := R.\sigma.\gamma.$$

For simplicity, we will write $\{\alpha\}$, $[\alpha]$ for $\{\mid \alpha \mid\}$ and $[\mid \alpha \mid]$, respectively, where $\mid \alpha \mid$ is the diagonal probabilistic relation induced by probabilistic predicate α. If $\alpha : \mathbf{P}\Sigma$, then for any $\beta : \mathbf{P}\Sigma$ and $\sigma : \Sigma$,

$$\{\alpha\}.\beta = \alpha \times \beta$$

and

$$[\alpha].\beta.\sigma = \min\left(1, \frac{\beta.\sigma}{\alpha.\sigma}\right).$$

The following two propositions present the congruence (or substitution) properties of probabilistic updates under some operations of probabilistic relations.

Proposition 6. *Let Σ, Γ and Δ be state spaces, and let $P : \Sigma \leftrightarrow \Gamma$ and $Q : \Gamma \leftrightarrow \Delta$. Then*
(1) $\{P \circ Q\} = \{P\}; \{Q\}$.
(2) $[P \circ Q] = [P]; [Q]$ if $P.\sigma.\gamma \leq 1$ for all $\sigma : \Sigma$ and $\gamma : \Gamma$.

Proof. We only prove (2), and the proof of (1) is easier. First, for any $\alpha : \mathbf{P}\Delta$ and $\sigma : \Sigma$ we have

$$\begin{aligned}
&([P]; [Q]).\alpha.\sigma = [P].([Q].\alpha).\sigma \\
&= \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{[Q].\alpha.\gamma}{P.\sigma.\gamma}\right)\right) \\
&= \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{(\sqcap\delta : \Delta \cdot \min(1, \frac{\alpha.\delta}{Q.\gamma.\delta}))}{P.\sigma.\gamma}\right)\right) \\
&= \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \left(\sqcap\delta : \Delta \cdot \min\left(\frac{1}{P.\sigma.\gamma}, \frac{\alpha.\delta}{P.\sigma.\gamma \times Q.\gamma.\delta}\right)\right)\right)\right) \\
&= \left(\sqcap\gamma : \Gamma \cdot \sqcap\delta : \Delta \cdot \min\left(1, \frac{1}{P.\sigma.\gamma}, \frac{\alpha.\delta}{P.\sigma.\gamma \times Q.\gamma.\delta}\right)\right).
\end{aligned}$$

Since $P.\sigma.\gamma \leq 1$, we have $\frac{1}{P.\sigma.\gamma} \geq 1$ and

$$([P];[Q]).\alpha.\sigma = \left(\sqcap\gamma : \Gamma \cdot \sqcap\delta : \Delta \cdot \min\left(1, \frac{\alpha.\delta}{P.\sigma.\gamma \times Q.\gamma.\delta}\right)\right)$$
$$= [P \circ Q].\alpha.\sigma.\#$$

We here give an example to show the necessity of the condition in Proposition 6(2) that P is bounded by 1. Suppose that $\Sigma = \Gamma = \Delta = \{\sigma\}$, $P.\sigma.\sigma = Q.\sigma.\sigma = 2$, and $\alpha.\sigma = 4$. Then a simple calculation shows that

$$[P \circ Q].\alpha.\sigma = 1 > \frac{1}{2} = ([P];[Q]).\alpha.\sigma$$

and $[P \circ Q] \neq [P];[Q]$.

The above proposition shows that the updates and the composition of probabilistic relations commute, whereas the next proposition indicates that the angelic update preserves unions of probabilistic relations, and the demonic update changes a union of probabilistic relations into a meet.

Proposition 7. *Let Σ and Γ be two state spaces, and let $R_i\ (i \in I) : \Sigma \leftrightarrow \Gamma$. If $(\sqcup i \in I \cdot R_i)$ is well-defined, then*
(1) $\{(\sqcup i \in I \cdot R_i)\} = (\sqcup i \in I \cdot \{R_i\})$, and
(2) $[(\sqcup i \in I \cdot R_i)] = (\sqcap i \in I \cdot [R_i])$.

Proof. By a simple calculation.#

4 Monotonicity

R. -J. Back and J. von Wright [2, 3, 45] discovered a very interesting theorem, called normal form theorem, which says that all monotone predicate transformers can be represented in terms of angelic and demonic updates (see also [4], Sect. 13.3 for an elegant exposition). It is known that the predicate transformers generated from the basic program constructs such as asserts, guards, functional updates, angelic and demonic updates, and angelic and demonic choices are all monotone. Conversely, the normal form theorem indicates that any monotone predicate transformers can be induced from the basic program constructs of angelic and demonic updates. So, the normal form theorem is very important for the theoretical analysis of sequential programming languages. In the realm of probabilistic programming, in order to clarify the structure of probabilistic predicate transformers, we certainly hope to find a probabilistic generalization of the normal form theorem. As will be illustrated by an example after Definition 8 together with Theorem 12, the concept of monotonicity given in Definition 1(2) is too weak to establish a normal form theorem, and we need a stronger notion of monotonicity

for probabilistic predicate transformers, which is in turn based on a notion of probabilistic implication strength. In a sense, probabilistic implication strength is a relativization and a further "probabilization" of probabilistic implication $\equiv>$.

Definition 7. *Let Σ be a state space and $\alpha, \beta : \mathbf{P}\Sigma$. Then the strength that α implies β is defined as*

$$\lceil \alpha \equiv> \beta \rceil := \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{\beta.\sigma}{\alpha.\sigma}\right)\right).$$

The notion of implication strength defined above is closely related to probabilistic implication. Indeed, it is easy to see that $\lceil \alpha \equiv> \beta \rceil = 1$ if and only if $\alpha \equiv> \beta$. However, implication strength is a much subtler concept than probabilistic implication. For instance, let $\Sigma =$ the non-negative integers, and let $\alpha.0 = 1 + 10^{-1000}$, $\alpha.\sigma = \frac{1}{2}$ for all $\sigma > 0$, and $\beta.\sigma = 1$ for all $\sigma : \Sigma$. Then $\alpha.\sigma < \beta.\sigma$ for all $\sigma : \Sigma$ except 0, and at the point 0, $\alpha.0$ is greater than $\beta.0$, but the difference is very small. Obviously, it does not hold that $\alpha \equiv> \beta$. In other words, $\alpha \equiv> \beta$ is absolutely a false statement. This is not reasonable since the difference between $\alpha.0$ and $\beta.0$ is small enough. On the other hand,

$$\lceil \alpha \equiv> \beta \rceil = \frac{10^{1000}}{10^{1000} + 1}$$

is very close to 1. This means that although α does not absolutely imply β, α implies β with a very high belief degree (or probability). Such a conclusion fits our intuition very well. With this observation, we know that probabilistic implication is a notion in two-valued logic, whereas implication strength is one in probabilistic logic.

A further link between probabilistic implication and implication strength is represented by the following Galois connection: for any $k \in [0, 1]$ and for all $\alpha, \beta : \mathbf{P}\Sigma$,

$$k \leq \lceil \alpha \equiv> \beta \rceil \text{ if and only if } k \times \alpha \equiv> \beta.$$

We define two auxiliary mappings $\lceil \alpha \equiv> \cdot \rceil : \mathbf{P}\Sigma \to [0, 1]$ and $\alpha^* : [0, 1] \to \mathbf{P}\Sigma$ as follows: for any $\beta : \mathbf{P}\Sigma$ and $k \in [0, 1]$,

$$\lceil \alpha \equiv> \cdot \rceil.\beta := \lceil \alpha \equiv> \beta \rceil,$$
$$(\alpha^*).k := k \times \alpha.$$

Then the link can be written more in the Galois style:

$$k \leq \lceil \alpha \equiv> \cdot \rceil.\beta \text{ if and only if } (\alpha^*).k \leq \beta.$$

This gives explicitly a Galois connection between the two mappings $\lceil \alpha \equiv > \cdot \rceil$ and α^*. The power of this Galois connection could be exploited to simplify considerably the proofs of some results.

The following two propositions provide us with some fundamental properties of implication strength. Proposition 8(1) states that implication strength is transitive, and Propositions 8(2)–(6) and 9 present a certain substitution (congruence) property, that is, implication strength is preserved by scale product, addition, subtraction, union, meet, and relation inverse and composition.

Proposition 8. *Let Σ be a state space, and let $\alpha, \beta, \gamma, \alpha_i, \beta_i$ $(i \in I) : \mathbf{P}\Sigma$. Then*
(1) $\lceil \alpha \equiv > \beta \rceil \times \lceil \beta \equiv > \gamma \rceil \leq \lceil \alpha \equiv > \gamma \rceil$.
(2) $\min(1, \frac{b}{a}) \times \lceil \alpha \equiv > \beta \rceil \leq \lceil a \times \alpha \equiv > b \times \beta \rceil$ *where* $a, b \in \mathbf{R}_{\geq}$.
(3) $\min(\lceil \alpha \equiv > \beta \rceil, \lceil \alpha' \equiv > \beta' \rceil) \leq \lceil \alpha + \alpha' \equiv > \beta + \beta' \rceil$.
(4) $\lceil \alpha \ominus \gamma \equiv > \beta \ominus \gamma \rceil \leq \lceil \alpha \equiv > \beta \rceil$ *if for all* $\sigma : \Sigma$, *we have* $\beta.\sigma \geq \alpha.\sigma$ *or* $\alpha.\sigma > \gamma.\sigma$.
(5) $(\sqcap i \in I \cdot \lceil \alpha_i \equiv > \beta_i \rceil) \leq \lceil (\sqcup i \in I \cdot \alpha_i) \equiv > (\sqcup i \in I \cdot \beta_i) \rceil$ *if* $(\sqcup i \in I \cdot \alpha_i)$ *and* $(\sqcup i \in I \cdot \beta_i)$ *exist.*
(6) $(\sqcap i \in I \cdot \lceil \alpha_i \equiv > \beta_i \rceil) \leq \lceil (\sqcap i \in I \cdot \alpha_i) \equiv > (\sqcap i \in I \cdot \beta_i) \rceil$.

Proof. We only demonstrate (1), (3), (4) and (5), and (2) and (6) are similar.
(1) It holds that

$$\begin{aligned}
&\lceil \alpha \equiv > \beta \rceil \times \lceil \beta \equiv > \gamma \rceil \\
&\quad = \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{\beta.\sigma}{\alpha.\sigma}\right)\right) \times \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{\gamma.\sigma}{\beta.\sigma}\right)\right) \\
&\quad \leq \left(\sqcap \sigma : \Sigma \cdot \min\left[1, \frac{\beta.\sigma}{\alpha.\sigma} \times \left(\sqcap \sigma' : \Sigma \cdot \min\left(1, \frac{\gamma.\sigma'}{\beta.\sigma'}\right)\right)\right]\right) \\
&\quad \leq \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{\beta.\sigma}{\alpha.\sigma} \times \frac{\gamma.\sigma}{\beta.\sigma}\right)\right) \\
&\quad = \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{\gamma.\sigma}{\alpha.\sigma}\right)\right) \\
&\quad = \lceil \alpha \equiv > \gamma \rceil.
\end{aligned}$$

(3) We write

$$\lambda = \min\left(\lceil \alpha \equiv > \beta \rceil, \lceil \alpha' \equiv > \beta' \rceil\right).$$

Then

$$\lambda \leq \lceil \alpha \equiv > \beta \rceil = \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{\beta.\sigma}{\alpha.\sigma}\right)\right)$$

and

$$\lambda \leq \lceil \alpha' \equiv > \beta' \rceil = \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{\beta'.\sigma}{\alpha'.\sigma}\right)\right).$$

This yields

$$\lambda \times \alpha.\sigma \leq \beta.\sigma,$$
$$\lambda \times \alpha'.\sigma \leq \beta'.\sigma,$$
$$\lambda \times (\alpha + \alpha').\sigma = \lambda \times \alpha.\sigma + \lambda \times \alpha'.\sigma \leq \beta.\sigma + \beta'.\sigma$$

for all $\sigma : \Sigma$, and further

$$\lambda \leq \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{(\beta + \beta').\sigma}{(\alpha + \alpha').\sigma}\right)\right) = \lceil \alpha + \alpha' \equiv> \beta + \beta' \rceil.$$

(4) We first have

$$\lceil \alpha \ominus \gamma \equiv > \beta \ominus \gamma \rceil = \Bigg(\sqcap \sigma : \Sigma \mid \max(0, \alpha.\sigma - \gamma.\sigma) \geq \max(0, \beta.\sigma - \gamma.\sigma) \cdot \frac{\max(0, \beta.\sigma - \gamma.\sigma)}{\max(0, \alpha.\sigma - \gamma.\sigma)} \Bigg).$$

It is easy to see that $\alpha.\sigma \geq \beta.\sigma$ implies

$$\max(0, \alpha.\sigma - \gamma.\sigma) \geq \max(0, \beta.\sigma - \gamma.\sigma).$$

This yields

$$\lceil \alpha \ominus \gamma \equiv> \beta \ominus \gamma \rceil \leq \left(\sqcap \sigma : \Sigma \mid \alpha.\sigma \geq \beta.\sigma \cdot \frac{\max(0, \beta.\sigma - \gamma.\sigma)}{\max(0, \alpha.\sigma - \gamma.\sigma)}\right).$$

Note that $\beta.\sigma \geq \alpha.\sigma$ or $\alpha.\sigma > \gamma.\sigma$ for all $\sigma : \Sigma$. We know that

$$\frac{\max(0, \beta.\sigma - \gamma.\sigma)}{\max(0, \alpha.\sigma - \gamma.\sigma)} \leq \frac{\beta.\sigma}{\alpha.\sigma}$$

whenever $\alpha.\sigma \geq \beta.\sigma$. Therefore,

$$\lceil \alpha \ominus \gamma \equiv> \beta \ominus \gamma \rceil \leq \left(\sqcap \sigma : \Sigma \mid \alpha.\sigma \geq \beta.\sigma \cdot \frac{\beta.\sigma}{\alpha.\sigma}\right) = \lceil \alpha \equiv> \beta \rceil.$$

(5) It holds that

$$\begin{aligned}
&\lceil (\sqcup i \in I \cdot \alpha_i) \equiv > (\sqcup i \in I \cdot \beta_i) \rceil \\
&\quad = \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{(\sqcup i \in I \cdot \beta_i.\sigma)}{(\sqcup i \in I \cdot \alpha_i.\sigma)}\right)\right) \\
&\quad = \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \left(\sqcap i \in I \cdot \frac{(\sqcup i' \in I \cdot \beta_{i'}.\sigma)}{\alpha_i.\sigma}\right)\right)\right) \\
&\quad \geq \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \left(\sqcap i \in I \cdot \frac{\beta_i.\sigma}{\alpha_i.\sigma}\right)\right)\right) \\
&\quad = \left(\sqcap i \in I \cdot \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{\beta}{\alpha_i.\sigma}\right)\right)\right) \\
&\quad = (\sqcap i \in I \cdot \lceil \alpha_i \equiv> \beta_i \rceil).\#
\end{aligned}$$

We have a simple example showing that the condition of Proposition 6(4) cannot be cancelled. Let $\Sigma = \{\sigma\}$, $\alpha.\sigma = \gamma.\sigma = 2$ and $\beta.\sigma = 1$. Then

$$\lceil \alpha \ominus \gamma \equiv> \beta \ominus \gamma \rceil = 1 > \frac{1}{2} = \lceil \alpha \equiv> \beta \rceil.$$

Proposition 9. *Let Σ, Γ and Δ be state spaces, $P, P' : \Sigma \leftrightarrow \Gamma$ and $Q, Q' : \Gamma \leftrightarrow \Delta$. Then*

$$\lceil P \equiv> P' \rceil \times \lceil Q \equiv> Q' \rceil \leq \lceil P \circ Q \equiv> P' \circ Q' \rceil.$$

Proof. This may be carried out with a combination of the arguments used in the proofs of Propositions 8(1) and (2).#

We may further expect that reflexive and transitive closure preserves implication strength, i.e., $\lceil P \equiv> Q \rceil \leq \lceil P^* \equiv> Q^* \rceil$. Unfortunately, it is not the case in general. It is obvious that $P \equiv> Q$ implies $P^* \equiv> Q^*$. Indeed, for any $\lambda < 1$, we can find probabilistic relations P and Q such that $\lceil P \equiv> Q \rceil = \lambda$ but $\lceil P^* \equiv> Q^* \rceil = 0$. Let $\Sigma =$ the non-negative integers. We define P and Q as follows:

$$\begin{cases} P.i.(i+1) = 1, & i = 0, 1, 2, ..., \\ P.i.j = 0 \quad \text{if } j \neq i+1, \end{cases}$$

and $Q = \lambda \times P$. Then it is clear that $\lceil P \equiv> Q \rceil = \lambda$. However, for any positive integer n,

$$\lceil P^* \equiv> Q^* \rceil \leq \frac{Q^*.0.n}{P^*.0.n} = \lambda^n.$$

This implies that $\lceil P^* \equiv> Q^* \rceil = 0$.

With the help of implication strength we are able to introduce the central notion of strong monotonicity in this section.

Definition 8. *Let Σ and Γ be two state spaces, and $t : \mathbf{\Sigma} \mapsto \mathbf{\Gamma}$. Then t is said to be strongly monotone if for all $\alpha, \beta : \mathbf{P\Gamma}$,*

$$\lceil \alpha \equiv> \beta \rceil \leq \lceil t.\alpha \equiv> t.\beta \rceil.$$

It is worth comparing the weak and strong monotonicity of probabilistic predicate transformers given in Definitions 1(2) and 8, respectively. The monotonicity of Boolean predicate transformer T may be defined by either

$$p \subseteq q \models T.p \subseteq T.q$$

or

$$\models p \subseteq q \Rightarrow T.p \subseteq T.q.$$

This is because the deduction theorem in two-valued logic assures that the above two logical statements are equivalent. However, the equivalence between them is no longer valid in a probabilistic logic. In other words, they are split into two different notions of monotonicity. It may be easily found that the notion of (weak) monotonicity is a "probabilization" of the former. In contrast, strong monotonicity is a "probabilization" of the latter. The following example illustrates further their difference: let $\Sigma = \{\sigma\}$ and $\Gamma = \{\gamma_1, \gamma_2\}$. The probabilistic predicate transformer $t : \Sigma \mapsto \Gamma$ is defined by

$$t.\alpha.\sigma = \alpha.\gamma_1 \times \alpha.\gamma_2$$

for any $\alpha : \mathbf{P}\Gamma$. Then t is monotone according to Definition 1(2). On the other hand, let $\alpha_1.\gamma_1 = \alpha_1.\gamma_2 = 2$ and $\alpha_2.\gamma_1 = \alpha_2.\gamma_2 = 1$. Then $t.\alpha_1.\sigma = 4$, $t.\alpha_2.\sigma = 1$ and

$$\lceil \alpha_1 \equiv\!> \alpha_2 \rceil = \frac{1}{2} > \frac{1}{4} = \lceil t.\alpha_1 \equiv\!> t.\alpha_2 \rceil.$$

This shows that t is not strongly monotone in the sense of Definition 8. Thus, the notion of strong monotonicity is really strictly stronger than the weak one. On the other hand, the following proposition shows that strong monotonicity can be derived from (weak) monotonicity plus the scaling property.

Proposition 10. *If $t : \Sigma \mapsto \Gamma$ is monotone and has the scaling property, i.e., $t.(a \times \alpha) \equiv a \times t.\alpha$ for all $a : \mathbf{R}_{\geq}$ and $\alpha : \mathbf{P}\Gamma$, then t is strongly monotone.*

Proof. For any $\alpha, \beta : \mathbf{P}\Gamma$, we first have $\lceil \alpha \equiv\!> \beta \rceil \times \alpha \equiv\!> \beta$. In fact, for any $\gamma : \Gamma$,

$$\begin{aligned}
&(\lceil \alpha \equiv\!> \beta \rceil \times \alpha).\gamma \leq \lceil \alpha \equiv\!> \beta \rceil \times \alpha.\gamma \\
&= \left(\sqcap \gamma' : \Gamma \cdot \min\left(1, \frac{\beta.\gamma'}{\alpha.\gamma'}\right)\right) \times \alpha.\gamma \\
&\leq \min\left(1, \frac{\beta.\gamma}{\alpha.\gamma}\right) \times \alpha.\gamma \\
&\leq \beta.\gamma.
\end{aligned}$$

Since t is monotone and scaling, it follows that

$$\lceil \alpha \equiv\!> \beta \rceil \times t.\alpha = t.(\lceil \alpha \equiv\!> \beta \rceil \times \alpha) \equiv\!> t.\beta.$$

Thus, for each $\sigma : \Sigma$,

$$\lceil \alpha \equiv\!> \beta \rceil \times t.\alpha.\sigma = (\lceil \alpha \equiv\!> \beta \rceil \times t.\alpha).\sigma \leq t.\beta.\sigma,$$

$$\lceil \alpha \equiv\!> \beta \rceil \leq \frac{t.\beta.\sigma}{t.\alpha.\sigma},$$

and

$$\lceil \alpha \equiv\!> \beta \rceil \leq \min\left(1, \frac{t.\beta.\sigma}{t.\alpha.\sigma}\right)$$

because it always holds that $\lceil \alpha \equiv\!> \beta \rceil \leq 1$. Let σ traverse the whole Σ. Then

$$\begin{aligned}\lceil \alpha \equiv\!> \beta \rceil &\leq \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{t.\beta.\sigma}{t.\alpha.\sigma}\right)\right) \\ &= \lceil t.\alpha \equiv\!> t.\beta \rceil,\end{aligned}$$

and t is strongly monotone.#

We now come to establish a normal form theorem for probabilistic predicate transformers. In order to do this, we first give a lemma which presents strong monotonicity of probabilistic updates as well as strong monotonicity preserved by basic operations of probabilistic predicate transformers.

Lemma 11. *(1) Let $R : \Sigma \leftrightarrow \Gamma$. Then $\{R\}$ and $[R]$ are strongly monotone probabilistic predicate transformers.*
(2) If $t_i\ (i \in I) : \Sigma \mapsto \Gamma$ are all strongly monotone, then $(\sqcap i \in I \cdot t_i)$ and $(\sqcup i \in I \cdot t_i)$ are also strongly monotone.
(3) If both $t_1 : \Sigma \mapsto \Gamma$ and $t_2 : \Gamma \mapsto \Delta$ are strongly monotone, then $t_1; t_2$ is also strongly monotone.

Proof. (1) We first deal with the angelic update. For any $\alpha, \beta : \mathbf{P}\Gamma$, it holds that

$$\begin{aligned}&\lceil \{R\}.\alpha \equiv\!> \{R\}.\beta \rceil = \left(\sqcap \sigma : \Sigma \cdot \min\left[1, \frac{(\sqcup \gamma : \Gamma \cdot R.\sigma.\gamma \times \alpha.\gamma)}{(\sqcup \gamma : \Gamma \cdot R.\sigma.\gamma \times \beta.\gamma)}\right]\right) \\ &= \left(\sqcap \sigma : \Sigma \cdot \min\left[1, \left(\sqcap \gamma' : \Gamma \cdot \frac{(\sqcup \gamma : \Gamma \cdot R.\sigma.\gamma \times \alpha.\gamma)}{R.\sigma.\gamma' \times \beta.\gamma'}\right)\right]\right) \\ &\geq \left(\sqcap \sigma : \Sigma \cdot \min\left[1, \left(\sqcap \gamma' : \Gamma \cdot \frac{R.\sigma.\gamma' \times \alpha.\gamma'}{R.\sigma.\gamma' \times \beta.\gamma'}\right)\right]\right) \\ &= \min\left[1, \left(\sqcap \gamma' : \Gamma \cdot \frac{\alpha.\gamma'}{\beta.\gamma'}\right)\right] \\ &= \left(\sqcap \gamma' : \Gamma \cdot \min\left(1, \frac{\alpha.\gamma'}{\beta.\gamma'}\right)\right) \\ &= \lceil \alpha \equiv\!> \beta \rceil.\end{aligned}$$

We now turn to consider demonic update. For any $\alpha, \beta : \mathbf{P}\Gamma$ and $\sigma : \Sigma$,

$$\frac{[R].\beta.\sigma}{[R].\alpha.\sigma} = \frac{\left(\sqcap \gamma : \Gamma . \min\left(1, \frac{\beta.\gamma}{R.\sigma.\gamma}\right)\right)}{\left(\sqcap \gamma : \Gamma . \min\left(1, \frac{\alpha.\gamma}{R.\sigma.\gamma}\right)\right)}$$

$$= \left(\sqcap \gamma' : \Gamma . \frac{\min\left(1, \frac{\beta.\gamma'}{R.\sigma.\gamma'}\right)}{\left(\sqcap \gamma : \Gamma . \min\left(1, \frac{\alpha.\gamma}{R.\sigma.\gamma}\right)\right)} \right).$$

We write $x = \min(1, \frac{\alpha.\gamma'}{R.\sigma.\gamma'})$. Then by noting that $x \leq \frac{\alpha.\gamma'}{R.\sigma.\gamma'}$ we have

$$\begin{aligned}
\frac{[R].\beta.\sigma}{[R].\alpha.\sigma} &\geq (\sqcap \gamma' : \Gamma . \frac{\min\left(1, \frac{\beta.\gamma'}{R.\sigma.\gamma'}\right)}{x})) \\
&= \left(\sqcap \gamma' : \Gamma . \min\left(\frac{1}{x}, \frac{\frac{\beta.\gamma'}{R.\sigma.\gamma'}}{x}\right)\right) \\
&\geq \left(\sqcap \gamma' : \Gamma . \min\left(\frac{1}{x}, \frac{\frac{\beta.\gamma'}{R.\sigma.\gamma'}}{\frac{\alpha.\gamma'}{R.\sigma.\gamma'}}\right)\right) \\
&= \left(\sqcap \gamma' : \Gamma . \min\left(\frac{1}{x}, \frac{\beta.\gamma'}{\alpha.\gamma'}\right)\right).
\end{aligned}$$

Furthermore, we obtain

$$\begin{aligned}
\lceil [R].\alpha \equiv> [R].\beta \rceil &= \left(\sqcap \sigma : \Sigma . \min\left(1, \frac{[R].\beta.\sigma}{[R].\alpha.\sigma}\right)\right) \\
&\geq \min\left[1, \left(\sqcap \gamma' : \Gamma . \min\left(\frac{1}{x}, \frac{\beta.\gamma'}{\alpha.\gamma'}\right)\right)\right] \\
&= \left(\sqcap \gamma' : \Gamma . \min\left(1, \frac{1}{x}, \frac{\beta.\gamma'}{\alpha.\gamma'}\right)\right) \\
&= \left(\sqcap \gamma' : \Gamma . \min\left(1, \frac{\beta.\gamma'}{\alpha.\gamma'}\right)\right) \\
&= \lceil \alpha \equiv> \beta \rceil
\end{aligned}$$

because $x \leq 1$.
(2) and (3) are immediate.#

Now we can present the main result of this section, namely normal form theorem for monotone probabilistic predicate transformers. This theorem is a generalization of Theorem 13.10 in [4], and it shows that any monotone probabilistic predicate transformer can be written as a statement term consisting of a probabilistic angelic update followed by a probabilistic demonic update.

Theorem 12. *Let Σ and Γ be state spaces and $t : \Sigma \mapsto \Gamma$. Then t is strongly monotone if and only if*

$$t = \{R\}; [R']$$

for some probabilistic relations R and R'.

Proof. ($\Leftarrow$) This is exactly the first and third parts of the above lemma.

($\Rightarrow$) We define probabilistic relations $R : \Sigma \times \mathbf{P}\Gamma \to [0,1]$ and $R' : \mathbf{P}\Gamma \times \Gamma \to [0,1]$ as follows:

$$.\sigma.\alpha := t.\alpha.\sigma,$$
$$R'.\alpha.\gamma := \alpha.\gamma$$

for all $\sigma : \Sigma$, $\gamma : \Gamma$ and $\alpha : \mathbf{P}\Gamma$. Then we have

$$\begin{aligned}
&(\{R\};[R']).\alpha.\sigma = (\sqcup\beta : \mathbf{P}\Gamma \cdot R.\sigma.\beta \times [R'].\alpha.\beta)\\
&= \left(\sqcup\beta : \mathbf{P}\Gamma \cdot t.\beta.\sigma \times \left(\sqcap\gamma : \Gamma \cdot \min\left[1, \frac{\alpha.\gamma}{R'.\beta.\gamma}\right]\right)\right)\\
&= \left(\sqcup\beta : \mathbf{P}\Gamma \cdot t.\beta.\sigma \times \left(\sqcap\gamma : \Gamma \cdot \min\left[1, \frac{\alpha.\gamma}{\beta.\gamma}\right]\right)\right)\\
&\geq t.\alpha.\sigma \times \left(\sqcap\gamma : \Gamma \cdot \min\left[1, \frac{\alpha.\gamma}{\alpha.\gamma}\right]\right)\\
&= t.\alpha.\sigma.
\end{aligned}$$

On the other hand, for any $\beta : \mathbf{P}\Gamma$, since t is a strongly monotone probabilistic predicate transformer, it follows that

$$\begin{aligned}
\left(\sqcap\gamma : \Gamma \cdot \min\left[1, \frac{\alpha.\gamma}{\beta.\gamma}\right]\right) &= \lceil \beta \equiv\!> \alpha \rceil\\
&\leq \lceil t.\beta \equiv\!> t.\alpha \rceil\\
&= \left(\sqcap\delta : \Sigma \cdot \min\left[1, \frac{t.\alpha.\delta}{t.\beta.\delta}\right]\right)\\
&\leq \frac{t.\alpha.\sigma}{t.\beta.\sigma},\\
t.\beta.\sigma \times \left(\sqcap\gamma : \Gamma \cdot \min\left[1, \frac{\alpha.\gamma}{\beta.\gamma}\right]\right) &\leq t.\alpha.\sigma,
\end{aligned}$$

and

$$\begin{aligned}
(\{R\};[R']).\alpha.\sigma &= \left(\sqcup\beta : \mathbf{P}\Gamma \cdot t.\beta.\sigma \times \left(\sqcap\gamma : \Gamma \cdot \min\left[1, \frac{\alpha.\gamma}{\beta.\gamma}\right]\right)\right)\\
&\leq t.\alpha.\sigma.
\end{aligned}$$

This together with the first inequality that we obtained yields $(\{R\};[R']).\alpha = t.\alpha.\#$

5 Conjunctivity, disjunctivity and continuity

It is not the case that all predicate transformers can serve as semantic interpretations of programming statements. According to E. W. Dijkstra [11], predicate transformers accepted as semantic functions of programming statements are required to satisfy certain healthiness conditions. Originally, he imposed strictness, conjunctivity and continuity. These restrictions describe some homomorphism properties of programs. Later, they have been weakened by some authors in order to strengthen the expressive power and to achieve algebraic simplicity. For example, monotonicity was introduced as a weakening of conjunctivity to accommodate the angelic abstraction statement [2-4]. On the other hand, some new healthiness conditions have been proposed. For instance, disjunctivity was used by W. H. Hesselink [16] in his study of command algebras.

The research on probabilistic healthiness was initiated by C. Morgan, A. McIver and K. Seidel [24, 29], and they considered the conditions of scaling, sub-additivity, additivity and $\ominus$-subdistribution. These restrictions characterize properly some important subclasses of probabilistic programs. One of the main topics of this paper is also healthiness conditions for probabilistic programs. The previous section was devoted to a thorough study of strong monotonicity. In this section, we continue our discussion of probabilistic healthiness and consider conjunctivity, disjunctivity and continuity. One interesting thing is that disjunctivity will split into two nonequivalent versions in the realm of probabilistic programming.

In a sense, additivity introduced in [24, 29] is a probabilistic version of disjunctivity. We first observe that sub-additivity implies (weak) monotonicity. In fact, if $\alpha \equiv> \beta$, then $\beta \ominus \alpha$ is a probabilistic predicate whether $\alpha \equiv> \beta$ or not (see [29]), and

$$t.\beta \equiv t.(\alpha + (\beta \ominus \alpha)) <\equiv t.\alpha + t.(\beta \ominus \alpha) \geq t.\alpha.$$

Furthermore, we note that additivity implies the scaling properties.

Lemma 13. *Let Σ and Γ be state spaces and $t : \Sigma \mapsto \Gamma$. If t is additive, i.e., $t.(\alpha + \alpha') \equiv t.\alpha + t.\alpha'$ for all $\alpha, \alpha' : \mathbf{P}\Gamma$, then it is also scaling, i.e., $t.(a \times \alpha) \equiv a \times t.\alpha$ for all $a : \mathbf{R}_{\geq}$ and $\alpha : \mathbf{P}\Gamma$.*

Proof. From additivity it is easy to show that $t.(n \times \alpha) \equiv n \times t.\alpha$ for each positive integer n. In addition, $t.(\underline{0}) \equiv t.(2 \times \underline{0}) \equiv 2 \times t.\underline{0}$. This implies $t.(0 \times \alpha) \equiv t.\underline{0} \equiv \underline{0} \equiv 0 \times t.\alpha$. If n is a positive integer, then

$$t.\alpha \equiv t.\left(n \times \left(\frac{1}{n} \times \alpha\right)\right) \equiv n \times t.\left(\frac{1}{n} \times \alpha\right)$$

and $t.(\frac{1}{n} \times \alpha) \equiv \frac{1}{n} \times t.\alpha$. Furthermore, for any non-negative integer m,

$$t.\left(\frac{m}{n} \times \alpha\right) \equiv t\left(m \times \left(\frac{1}{n} \times \alpha\right)\right)$$
$$\equiv m \times t.\left(\frac{1}{n} \times \alpha\right) \equiv m \times \frac{1}{n} \times t.\alpha \equiv \frac{m}{n} \times t.\alpha.$$

This means that for all non-negative rational number r, it holds that $t.(r \times \alpha) \equiv r \times t.\alpha$. Now let $a \in R_{\geq}$. There should be two sequences $\{r_n^{(1)}\}$ and $\{r_n^{(2)}\}$ of non-negative rational numbers such that $\{r_n^{(1)}\}$ is increasing, $\{r_n^{(2)}\}$ is decreasing and $\lim_{n\to\infty} r_n^{(1)} = \lim_{n\to\infty} r_n^{(2)} = a$. Then from monotonicity of t it follows that

$$r_n^{(1)} \times \alpha \equiv\!> a \times \alpha \equiv\!> r_n^{(2)} \times \alpha,$$
$$r_n^{(1)} \times t.\alpha \equiv t.(r_n^{(1)} \times \alpha) \equiv\!> t.(a \times \alpha) \equiv\!> t.(r_n^{(2)} \times \alpha) \equiv r_n^{(2)} \times t.\alpha$$

and

$$t.(a \times \alpha) \equiv \lim_{n\to\infty}(r_n^{(1)} \times t.\alpha) \equiv \lim_{n\to\infty}(r_n^{(2)} \times t.\alpha) \equiv a \times t.\alpha.\#$$

We already knew that monotonicity may be derived from sub-additivity. In general, however, additivity does not imply strong monotonicity. For the case of finite state space, we have:

Proposition 14. *Let Σ and Γ be state spaces and $t : \Sigma \mapsto \Gamma$. If Γ is finite and t is additive, then t is strongly monotone.*

Proof. Since Γ is finite, for each $\alpha : \mathbf{P}\Gamma$, we can write

$$\alpha \equiv (\Sigma_{\gamma:\Gamma}\alpha.\gamma \times \overline{\gamma}).$$

It is supposed that t is additive. The above lemma asserts that t is scaling. Thus,

$$t.\alpha = (\Sigma_{\gamma:\Gamma}\alpha.\gamma \times t.\overline{\gamma}).$$

Now let $\alpha, \beta : \mathbf{P}\Gamma$. Then we may use Propositions 8(2) and (3) to obtain that

$$\begin{aligned}
\lceil t.\alpha \equiv\!> t.\beta\rceil &= \lceil(\Sigma_{\gamma:\Gamma}\alpha.\gamma \times t.\overline{\gamma}) \equiv\!> (\Sigma_{\gamma:\Gamma}\beta.\gamma \times t.\overline{\gamma})\rceil \\
&\geq (\sqcap\gamma : \Gamma \cdot \lceil\alpha.\gamma \times t.\overline{\gamma} \equiv\!> \beta.\gamma \times t.\overline{\gamma}\rceil) \\
&\geq \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{\beta.\gamma}{\alpha.\gamma}\right) \times \lceil t.\overline{\gamma} \equiv\!> t.\overline{\gamma}\rceil\right) \\
&= \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{\beta.\gamma}{\alpha.\gamma}\right)\right) \\
&= \lceil\alpha \equiv\!> \beta\rceil.\#
\end{aligned}$$

We now turn to introduce another version of probabilistic disjunctivity, and we also propose the notion of conjunctivity for probabilistic predicate transformers.

Definition 9. *Let Σ and Γ be two state spaces and $t : \Sigma \mapsto \Gamma$.*
(1) t is strict if $t.false = false$, where the $false$ in the left-hand side is the bottom element of $\mathbf{P}\Gamma$ and the $false$ in the right-hand side the bottom of $\mathbf{P}\Sigma$.
(2) t is conjunctive if $t.(\sqcap i \in I \cdot \alpha_i) = (\sqcap i \in I \cdot t.\alpha_i)$ for any non-empty family $\{\alpha_i \mid i \in I\}$ of probabilistic predicates on Γ.
(3) t is disjunctive if $t.(\sqcup i \in I \cdot \alpha_i) = (\sqcup i \in I \cdot t.\alpha_i)$ whenever $(\sqcup i \in I \cdot \alpha_i)$ is well-defined.
(4) t is said to be universally disjunctive if t is both strict and disjunctive.

Obviously, a conjunctive or disjunctive probabilistic predicate transformer is monotone. But neither conjunctivity nor disjunctivity imply strong monotonicity. The following proposition indicates that strong monotonicity is implied by conjunctivity or disjunctivity together with the scaling property.

Proposition 15. *Let Σ and Γ be state spaces. If $t : \Sigma \mapsto \Gamma$ is disjunctive (or conjunctive) and it satisfies the scaling property, then t is strongly monotone.*

Proof. It is immediate from Proposition 10 and the (weak) monotonicity of disjunctive (or conjunctive) probabilistic predicate transformers.#

For the case of disjunctivity, we can also prove the above proposition in a way similar to the proof of Proposition 14. The only difference is that a probabilistic predicate transformer α on Γ is decomposed to an angelic choice:

$$\alpha = (\sqcup \gamma : \Gamma \cdot \alpha.\gamma \times \overline{\gamma})$$

instead of a summation. For conjunctivity, the scaling property in the above proposition may be replaced by a local monotonicity. In other words, conjunctivity is able to extend a local monotonicity to a global one. In order to express this fact more precisely, we introduce the following

Definition 10. *(1) Let $\gamma : \Gamma$ and $M, \lambda : \mathbf{R}_{\geq}$. We define $\gamma_{M,\lambda} : \mathbf{P}\Gamma$ by*

$$\gamma_{M,\lambda}.\gamma' = \begin{cases} \lambda \text{ if } \gamma' = \gamma, \\ M \text{ otherwise.} \end{cases}$$

(2) Let $t : \Sigma \mapsto \Gamma$. If for any $\gamma : \Gamma$ and $M, \lambda : \mathbf{R}_{\geq}$, it holds that

$$\text{(LSM)} \qquad \frac{\lambda_1}{\lambda_2} \leq \lceil t.\gamma_{M,\lambda_2} \equiv\!> t.\gamma_{M,\lambda_1} \rceil,$$

then t is said to be locally strongly monotone.

For any $\gamma : \Gamma$ and $M, \lambda_1, \lambda_2 : \mathbf{R}_{\geq}$, if $\lambda_1 < \lambda_2 < M$, then

$$\lceil \gamma_{M,\lambda_2} \equiv\!> \gamma_{M,\lambda_1} \rceil = \frac{\lambda_1}{\lambda_2}.$$

This tells us that strong monotonicity of t implies its local strong monotonicity. Conversely, we have:

Proposition 16. *Let $t : \Sigma \mapsto \Gamma$ be conjunctive. If t satisfies the local strong monotonicity (LSM), then t is strongly monotone.*

Proof. For any $\alpha, \beta : \mathbf{P}\Gamma$, since they are all bounded, we can find $M : \mathbf{R}_{\geq}$ such that $\alpha.\gamma < M$ and $\beta.\gamma < M$ for all $\gamma : \Gamma$. Moreover, α and β may be expressed as

$$\alpha = (\sqcap \gamma : \Gamma \cdot \gamma_{M,\alpha.\gamma})$$

and

$$\beta = (\sqcap \gamma : \Gamma \cdot \gamma_{M,\beta.\gamma}).$$

By using conjunctivity of t we assert that

$$t.\alpha = (\sqcap \gamma : \Gamma \cdot t.\gamma_{M,\alpha.\gamma})$$

and

$$t.\beta = (\sqcap \gamma : \Gamma \cdot t.\gamma_{M,\beta.\gamma}).$$

Consequently,

$$\begin{aligned} \lceil t.\alpha \equiv\!> t.\beta \rceil &= \lceil (\sqcap \gamma : \Gamma \cdot t.\gamma_{M,\alpha.\gamma}) \equiv\!> (\sqcap \gamma : \Gamma \cdot t.\gamma_{M,\beta.\gamma}) \rceil \\ &\geq (\sqcap \gamma : \Gamma \cdot \lceil t.\gamma_{M,\alpha.\gamma} \equiv\!> t.\gamma_{M,\beta.\gamma} \rceil), \end{aligned}$$

where Proposition 8(6) is used to derive the last inequality. If $\alpha.\gamma \leq \beta.\gamma$, then

$$\gamma_{M,\alpha.\gamma} \equiv\!> \gamma_{M,\beta.\gamma}.$$

Noting that conjunctivity implies monotonicity, we have

$$t.\gamma_{M,\alpha.\gamma} \equiv\!> t.\gamma_{M,\beta.\gamma}$$

and

$$\lceil t.\gamma_{M,\alpha.\gamma} \equiv\!> t.\gamma_{M,\beta.\gamma} \rceil = 1.$$

For the case of $\alpha.\gamma > \beta.\gamma$, the local strong monotonicity of t leads to

$$\frac{\beta.\gamma}{\alpha.\gamma} \leq \lceil t.\gamma_{M,\alpha.\gamma} \equiv\!> t.\gamma_{M,\beta.\gamma} \rceil.$$

Therefore,

$$\lceil t.\alpha \equiv\!> t.\beta \rceil \geq \left(\sqcap \gamma : \Gamma \cdot \min\left(1, \frac{\beta.\gamma}{\alpha.\gamma}\right)\right)$$

$$= \lceil \alpha \equiv\!> \beta \rceil.\#$$

The disjunctivity for probabilistic predicate transformers introduced in Definition 9 is a direct generalization of its non-probabilistic cousin (see [4], page 260). On the other hand, sub-additivity is also a probabilistic analog of non-probabilistic disjunctivity. The following proposition describes the overlap of sub-additivity and disjunctivity. It can be seen that transformers satisfying both disjunctivity and sub-additivity are sparse in the whole space of probabilistic predicate transformers. In other words, disjunctivity and sub-additivity contradict each other to a certain extent.

Proposition 17. *Let Γ be a finite state space and $t : \Sigma \to \Gamma$. If t is both sub-additive and disjunctive, then there is a family γ_σ $(\sigma \in \Sigma)$ of elements in Γ indexed by Σ such that for all $\alpha : \mathbf{P}\Gamma$ and $\sigma : \Sigma$,*

$$t.\alpha.\sigma = t.(\alpha.\gamma_\sigma \times \overline{\gamma_\sigma}).\sigma.$$

Proof. We first prove the following auxiliary result.

Claim 1. Let $\{r_i \mid i \in I\}$ be a finite set of non-negative reals. If

$$(\sqcup i \in I \cdot r_i) = \Sigma_{i \in I} r_i < \infty,$$

then there is at most one i_0 in I such that $r_{i_0} > 0$.

We write $M = (\sqcup i \in I \cdot r_i)$. Indeed, if $M = 0$, it is clear. We now assume that $M > 0$. Then there should be some $i_0 \in I$ with $r_{i_0} > 0$, and we consider the following two cases:

Case 1. $r_{i_0} = M$. In this case, for each $i \in I - \{i_0\}$, we have

$$r_i \leq \Sigma_{i \neq i_0} r_i = M - r_{i_0} = 0.$$

Case 2. $r_{i_0} < M$. There is a positive integer n_0 such that $r_{i_0} < M - \frac{1}{n_0}$. In addition, since $r_{i_0} > 0$, we have some positive integer n_1 with $\frac{1}{n_1} < r_{i_0}$. Let $n = \max(n_0, n_1)$. Then $\frac{1}{n} < r_{i_0}$ and $r_{i_0} < M - \frac{1}{n}$. On the other hand, there must be some $i_1 \in I$ with $r_{i_1} > M - \frac{1}{n}$ because $M = (\sqcup i \in I \cdot r_i)$. From $r_{i_1} > M - \frac{1}{n}$ and $r_{i_0} < M - \frac{1}{n}$, we know that $i_0 \neq i_1$. Thus,

$$\Sigma_{i \in I} r_i \geq r_{i_0} + r_{i_1} > \frac{1}{n} + \left(M - \frac{1}{n}\right) = M,$$

a contradiction.

With the above auxiliary conclusion, we now are able to prove the proposition. For any $M \in R_{\geq}$, finiteness of P allows us to write

$$\overline{M} \equiv \Sigma_{\gamma:\Gamma}(M \times \overline{\gamma}) \equiv (\sqcup\gamma : \Gamma \cdot M \times \overline{\gamma}).$$

Then sub-additivity and disjunctivity of t leads to

$$\Sigma_{\gamma:\Gamma} t.(M \times \overline{\gamma}) \equiv> t.\overline{M} \equiv (\sqcup\gamma : \Gamma \cdot t.(M \times \overline{\gamma})).$$

Now for each $\sigma : \Sigma$, we have

$$\Sigma_{\gamma:\Gamma} t.(M \times \overline{\gamma}).\sigma \leq t.\overline{M}.\sigma \equiv (\sqcup\gamma : \Gamma \cdot t.(M \times \overline{\gamma}).\sigma).$$

With Claim 1 we know that there is at most one $\gamma_{M,\sigma}$ in Γ such that $t.(M \times \overline{\gamma_{M,\sigma}}).\sigma > 0$.

Claim 2. $\gamma_{M,\sigma}$ is independent of M, i.e., $\gamma_{M_1,\sigma} = \gamma_{M_2,\sigma}$ for all $M_1, M_2 : R_{\geq}$ and $\sigma : \Sigma$.

In fact, if $M_1 < M_2$ and $\gamma_{M_1,\sigma} \neq \gamma_{M_2,\sigma}$, then

$$M_1 \times \overline{\gamma_{M_1,\sigma}} \equiv> M_2 \times \overline{\gamma_{M_2,\sigma}}.$$

Since t is disjunctive, it is also monotone, and

$$\begin{aligned} t.(M_1 \times \overline{\gamma_{M_1,\sigma}}) &\equiv > t.(M_2 \times \overline{\gamma_{M_2,\sigma}}), \\ 0 < t.(M_1 \times \overline{\gamma_{M_1,\sigma}}).\sigma &\leq t.(M_2 \times \overline{\gamma_{M_2,\sigma}}).\sigma. \end{aligned}$$

This contradicts the uniqueness of $\gamma_{M_2,\sigma}$.

From Claim 2, it follows that for any $\sigma : \Sigma$, there exists $\gamma_\sigma : \Gamma$ such that $\gamma \neq \gamma_\sigma$ implies $t.(M \times \overline{\gamma}).\sigma = 0$ for all $M : R_{\geq}$. Therefore, disjunctivity of t yields

$$\begin{aligned} t.\alpha.\sigma &= t.(\sqcup\gamma : \Gamma \cdot \alpha.\gamma \times \overline{\gamma}).\sigma \\ &= (\sqcup\gamma : \Gamma \cdot t.(\alpha.\gamma \times \overline{\gamma}).\sigma) \\ &= t.(\alpha.\gamma_\sigma \times \overline{\gamma_\sigma}).\sigma.\# \end{aligned}$$

We now examine conjunctivity and disjunctivity of various probabilistic program constructs.

Proposition 18. *Let $R : \Sigma \leftrightarrow \Gamma$, $t_1, t_i\ (i \in I) : \Sigma \mapsto \Gamma$ and $t_2 : \Gamma \mapsto \Delta$. Then*
(1) $\{R\}$ is universally disjunctive and scaling.
(2) $[R]$ is conjunctive.
(3) if t_1 and t_2 are strict (resp. conjunctive, disjunctive, scaling, sub-additive, additive, $\ominus-$subdistributive), so is $t_1; t_2$.

(4) if t_i $(i \in I)$ are strict (resp. disjunctive, scaling, $\ominus-$subdistributive), so is $(\sqcup i \in I \cdot t_i)$ provided it is well-defined.
(5) if t_i $(i \in I)$ are conjunctive (resp. scaling, sub-additive, $\ominus-$subdistributive), so is $(\sqcap i \in I \cdot t_i)$.

Proof. Routine.#

The above proposition shows that probabilistic angelic update is disjunctive and scaling. Conversely, the following theorem gives a sufficient and necessary condition for a probabilistic predicate transformer to be an angelic update.

Theorem 19. Let Σ and Γ be state spaces and $t : \Sigma \mapsto \Gamma$. Then there is a (unique) $R : \Sigma \leftrightarrow \Gamma$ such that $t = \{R\}$ if and only if
(1) t is disjunctive and scaling, and
(2) there is $M : \mathbf{R}_{\geq}$ with $t.\overline{\gamma}.\sigma \leq M$ for all $\sigma : \Sigma$ and $\gamma : \Gamma$.

Proof. $(\Rightarrow)$ If $t = \{R\}$, then Proposition 18(1) gives the disjunctivity and scaling property of t. Since $R : \Sigma \leftrightarrow \Gamma$ is bounded, we can find some $M : \mathbf{R}_{\geq}$ with $R.\sigma.\gamma \leq M$ for any $\sigma : \Sigma$ and $\gamma : \Gamma$. Then

$$\begin{aligned} t.\overline{\gamma}.\sigma &= \{R\}.\overline{\gamma}.\sigma \\ &= (\sqcup\delta : \Gamma \cdot R.\sigma.\delta \times \overline{\gamma}.\delta) \\ &= R.\sigma.\gamma \leq M. \end{aligned}$$

$(\Leftarrow)$ Suppose that t satisfies the condition (1) and (2). For any $\sigma : \Sigma$ and $\gamma : \Gamma$, we define $R.\sigma.\gamma = t.\overline{\gamma}.\sigma$. Then the condition (2) implies that R is bounded and $R : \Sigma \leftrightarrow \Gamma$. Furthermore, using the condition (1) we obtain for any $\alpha : \mathbf{P}\Gamma$ and $\sigma : \Sigma$,

$$\begin{aligned} t.\alpha.\sigma &= (\sqcup\gamma : \Gamma \cdot \alpha.\gamma \times \overline{\gamma}).\sigma \\ &= (\sqcup\gamma : \Gamma \cdot t.(\alpha.\gamma \times \overline{\gamma})).\sigma \\ &= (\sqcup\gamma : \Gamma \cdot \alpha.\gamma \times t.\overline{\gamma}).\sigma \\ &= (\sqcup\gamma : \Gamma \cdot \alpha.\gamma \times t.\overline{\gamma}.\sigma) \\ &= (\sqcup\gamma : \Gamma \cdot R.\sigma.\gamma \times \alpha.\gamma) \\ &= \{R\}.\alpha.\sigma. \end{aligned}$$

The uniqueness of R is immediate from Proposition 27(2) below .#

Note that from the scaling property we have $t.false = false$. So, universal disjunctivity of t is a consequence of the assumption (1) in the above theorem, which generalizes R. -J. Back and J. von Wright's normal form theorem for non-probabilistic universally disjunctive predicate transformers ([4], Corollary 26.6). Furthermore, the following corollary may be seen as a probabilistic generalization of Corollary 26.8 in [4], i.e., the normal form theorem for disjunctive non-probabilistic predicate transformers.

Corollary 20. *If $t : \Sigma \mapsto \Gamma$ satisfies the following conditions:*
(1) $t.\alpha \equiv\!> \underline{1}$ for all $\alpha : \mathbf{P}\Gamma$,
(2) t is disjunctive, and
(3) t is weakly scaling in the sense that $t.(a \times \alpha) \equiv a \times t.\alpha$ for all $a > 0$ and $\alpha : \mathbf{P}\Gamma$, then there are $p : \mathbf{P}\Sigma$ and $R : \Sigma \leftrightarrow \Gamma$ such that $t = [p]; \{R\}$.

Proof. We define

$$p.\sigma = \begin{cases} 1 \text{ if } t.false.\sigma = 0, \\ 0 \text{ otherwise.} \end{cases}$$

Then using the condition (2) and Propositions 18(2) and (3) we know that $\{p\}; t$ is disjunctive; and from the condition (3) and Propositions 18(2) and (3) again we also know that $\{p\}; t$ is weakly scaling. In addition, it is easy to check that $(\{p\}; t).false \equiv false$. This together with weak scaling property entails obviously scaling property. We now can use Theorem 19 on $\{p\}; t$ to find some $R : \Sigma \leftrightarrow \Gamma$ such that $\{p\}; t = \{R\}$. Thus, $[p]; \{R\} = [p]; \{p\}; t$, and it suffices to show that $t = [p]; \{p\}; t$. This is immediate from the assumption (1).#

In the non-probabilistic case, the normal form theorem for universally conjunctive transformer may be easily derived by a duality argument from the one for universally disjunctive transformers and vice versa. Unfortunately, there is not a suitable duality between probabilistic universal conjunctivity and disjunctivity, and we have to adopt a direct approach to universally conjunctive probabilistic predicate transformers.

Theorem 21. *Let Σ and Γ be state spaces and $t : \Sigma \mapsto \Gamma$. Then*
(1) t is conjunctive and strongly monotone,
(2) $t.\underline{1} \equiv \overline{1}$,
(3) $t.\alpha \equiv\!> \underline{1}$ for all $\alpha : \mathbf{P}\Gamma$, and
(4) $t(\frac{\alpha}{t.\alpha.\sigma}).\sigma = 1$ for all $\alpha : \mathbf{P}\Gamma$ and $\sigma : \Sigma$
if and only if there exists a unique $R : \Sigma \leftrightarrow \Gamma$ such that
(a) $t = [R]$, and
(b) $R.\sigma.\gamma \leq 1$ for all $\sigma : \Sigma$ and $\gamma : \Gamma$.

Proof. ($\Rightarrow$) Suppose that t satisfies the conditions (1) through (4). Then we define:

$$R.\sigma.\gamma := \left(\sqcap \beta : \mathbf{P}\Gamma \cdot \min\left(1, \frac{\alpha.\gamma}{t.\beta.\sigma}\right)\right)$$

for all $\sigma : \Sigma$ and $\gamma : \Gamma$. From the above defining equation, it is easy to know that $R.\sigma.\gamma \leq 1$ for any $\sigma : \Sigma$ and $\gamma : \Gamma$. We now aim at proving that $t = [R]$. For each $\alpha : \mathbf{P}\Gamma$ and $\sigma : \Sigma$, with the definition of $R.\sigma.\gamma$ we have

$$R.\sigma.\gamma \leq \min\left(1, \frac{\alpha.\gamma}{t.\alpha.\sigma}\right) \leq \frac{\alpha.\gamma}{t.\alpha.\sigma},$$

and

$$\frac{\alpha.\gamma}{R.\sigma.\gamma} \geq \frac{\alpha.\gamma}{\frac{\alpha.\gamma}{t.\alpha.\sigma}} \geq t.\alpha.\sigma$$

for all $\gamma : \Gamma$. From the assumption (3) it follows that $t.\alpha.\sigma \leq 1$, and

$$t.\alpha.\sigma \leq \min\left(1, \frac{\alpha.\gamma}{R.\sigma.\gamma}\right).$$

Thus, noting that γ is arbitrary in the above inequality, we obtain

$$t.\alpha.\sigma \leq \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{\alpha.\gamma}{R.\sigma.\gamma}\right)\right) = [R].\alpha.\sigma.$$

To prove the reverse of the above inequality, we write $R.\sigma$ for the projection of R on Γ at σ, i.e., $R.\sigma$ is in $\mathbf{P}\Gamma$, and $(R.\sigma).\gamma := R.\sigma.\gamma$ for any $\gamma : \Gamma$. Then

$$R.\sigma = \left(\sqcap : \mathbf{P}\Gamma \cdot \left(\overline{1} \sqcap \frac{\beta}{t.\beta.\sigma}\right)\right),$$

and

$$\begin{aligned} t.(R.\sigma) &= \left(\sqcap\beta : \mathbf{P}\Gamma \cdot \left(t.\overline{1} \sqcap t.\left(\frac{\beta}{t.\beta.\sigma}\right)\right)\right) \\ &= \left(\sqcap\beta : \mathbf{P}\Gamma \cdot \left(\overline{1} \sqcap t.\left(\frac{\beta}{t.\beta.\sigma}\right)\right)\right) \\ &= \left(\sqcap\beta : \mathbf{P}\Gamma \cdot t.\left(\frac{\beta}{t.\beta.\sigma}\right)\right). \end{aligned}$$

The above three equality are derived by the assumption (1), (2), and (3), respectively. For any $\beta : \mathbf{P}\Gamma$, the assumption (4) asserts that

$$t\left(\frac{\beta}{t.\beta.\sigma}\right).\sigma = 1.$$

Thus,

$$t.(R.\sigma).\sigma = \left(\sqcap\beta : \mathbf{P}\Gamma \cdot t.(\frac{\beta}{t.\beta.\sigma}).\sigma\right) = 1.$$

Finally, with the strong monotonicity of t we have

$$\begin{aligned} [R].\alpha.\sigma &= \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{\alpha.\gamma}{R.\sigma.\gamma}\right)\right) \\ &= \lceil R.\sigma \equiv> \alpha \rceil \\ &\leq \lceil t.(R.\sigma) \equiv> t.\alpha \rceil \\ &= \left(\sqcap\delta : \Gamma \cdot \min\left(1, \frac{t.\alpha.\delta}{t.(R.\sigma).\delta}\right)\right) \\ &\leq \min\left(1, \frac{t.\alpha.\sigma}{t.(R.\sigma).\sigma}\right) \\ &= t.\alpha.\sigma. \end{aligned}$$

($\Leftarrow$) Assume that $R : \Sigma \leftrightarrow \Gamma$ satisfies $R.\sigma.\gamma \leq 1$ for all $\sigma : \Sigma$ and $\gamma : \Gamma$, and $t = [R]$. Then Propositions 18(2) and Lemma 11(1) tell us that t is conjunctive and strongly monotone. From the definition of $[R]$, it is clear that $t.\alpha.\sigma = [R].\alpha.\sigma \leq 1$ for all $\sigma : \Sigma$, i.e., $t.\alpha \equiv> \underline{1}$, and the condition (b) implies (2). Now it suffices to demonstrate the assertion (4). In fact, for any $\gamma : \Gamma$, we have

$$\begin{aligned} t.\alpha.\sigma \times R.\sigma.\gamma &= [R].\alpha.\sigma \times R.\sigma.\gamma \\ &= \left(\sqcap\delta : \Gamma \cdot \min\left(1, \frac{\alpha.\delta}{R.\sigma.\delta}\right)\right) \times R.\sigma.\gamma \\ &\leq \min\left(1, \frac{\alpha.\gamma}{R.\sigma.\gamma}\right) \times R.\sigma.\gamma \\ &\leq \frac{\alpha.\gamma}{R.\sigma.\gamma} \times R.\sigma.\gamma = \alpha.\gamma, \end{aligned}$$

and

$$\frac{\frac{\alpha.\gamma}{t.\alpha.\sigma}}{R.\sigma.\gamma} = \frac{\alpha.\gamma}{t.\alpha.\sigma \times R.\sigma.\gamma} \geq 1.$$

Hence,

$$\begin{aligned} t.\left(\frac{\alpha}{t.\alpha.\sigma}\right).\sigma &= [R].\left(\frac{\alpha}{t.\alpha.\sigma}\right).\sigma \\ &= \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{\frac{\alpha.\gamma}{t.\alpha.\sigma}}{R.\sigma.\gamma}\right)\right) = 1. \end{aligned}$$

Corollary 22. *Let $t : \Sigma \mapsto \Gamma$. Then there are $\alpha : \mathbf{P}\Sigma$ and $R : \Sigma \leftrightarrow \Gamma$ such that $t = \{\alpha\}; [R]$ and $R.\sigma.\gamma \leq 1$ for each $\sigma : \Sigma$ and $\gamma : \Gamma$ if and only if*
(1) t is conjunctive and strongly monotone,
(2) $t.\beta \equiv> t.\underline{1}$ for all $\beta : \mathbf{P}\Gamma$, and
(3) for any $\sigma : \Sigma$ and $\beta : \mathbf{P}\Gamma$, it holds that

$$t.\left(\beta \sqcup \frac{t.\underline{1}.\sigma \times \beta}{t.\beta.\sigma}\right).\sigma \geq t.\underline{1}.\sigma.$$

Proof. ($\Rightarrow$) If $t = \{\alpha\}; [R]$, then (1) is immediate from Lemmas 11(1) and (3) and Propositions 18(2) and (3), and (2) is easy and omitted. Now what remains is to demonstrate the inequality in (3). For any $\gamma : \Gamma$,

$$\begin{aligned} [R].\beta.\sigma \times \frac{R.\sigma.\gamma}{\beta.\gamma} &= \left(\sqcap\delta : \Gamma \cdot \min\left(1, \frac{\beta.\delta}{R.\sigma.\delta}\right)\right) \times \frac{R.\sigma.\gamma}{\beta.\gamma} \\ &\leq \min\left(1, \frac{\beta.\gamma}{R.\sigma.\gamma}\right) \times \frac{R.\sigma.\gamma}{\beta.\gamma} \leq 1. \end{aligned}$$

Then it follows that

$$[R].\beta.\sigma \times \frac{R.\sigma.\gamma}{\beta.\gamma} \times [R].\underline{1}.\sigma \leq [R].\underline{1}.\sigma \leq [R].\beta.\sigma \sqcup [R].\underline{1}.\sigma,$$

and

$$[R].\underline{1}.\sigma \leq \frac{\max\left(\beta.\gamma, \frac{[R].\underline{1}.\sigma \times \beta.\gamma}{[R].\beta.\sigma}\right)}{R.\sigma.\gamma} = \frac{\max\left(\beta.\gamma, \frac{t.\underline{1}.\sigma \times \beta.\gamma}{t.\beta.\sigma}\right)}{R.\sigma.\gamma}$$

because $t.\underline{1}.\sigma = \alpha.\sigma \times [R].\underline{1}.\sigma$ and $t.\beta.\sigma = \alpha.\sigma \times [R].\beta.\sigma$. Noting that $[R].\underline{1}.\sigma \leq 1$ always holds, we have

$$[R].\underline{1}.\sigma \leq \min\left(1, \frac{\max\left(\beta.\gamma, \frac{t.\underline{1}.\sigma \times \beta.\gamma}{t.\beta.\sigma}\right)}{R.\sigma.\gamma}\right).$$

Furthermore, arbitrariness of γ yields

$$[R].\underline{1}.\sigma \leq \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{\max\left(\beta.\gamma, \frac{t.\underline{1}.\sigma \times \beta.\gamma}{t.\beta.\sigma}\right)}{R.\sigma.\gamma}\right)\right) = [R].\left(\beta \sqcup \frac{t.\underline{1}.\sigma \times \beta}{t.\beta.\sigma}\right).\sigma.$$

Therefore,

$$\begin{aligned} t.\underline{1}.\sigma &= \alpha.\sigma \times [R].\underline{1}.\sigma \\ &\leq \alpha.\sigma \times [R].\left(\beta \sqcup \frac{t.\underline{1}.\sigma \times \beta}{t.\beta.\sigma}\right).\sigma \\ &= t.\left(\beta \sqcup \frac{t.\underline{1}.\sigma \times \beta}{t.\beta.\sigma}\right).\sigma. \end{aligned}$$

($\Leftarrow$) We put $t' = [t.\underline{1}].t$. It is clear that $t'.\beta \equiv> \underline{1}$ for all $\beta : \mathbf{P}\Gamma$, and $t'.\underline{1} = \underline{1}$. From Lemmas 11(1) and (3) and Propositions 18(2) and (3) it is easy to know that t' is also conjunctive and strongly monotone. For any $\beta : \mathbf{P}\Gamma$ and $\sigma : \Sigma$, from the assumption (3) we obtain

$$\begin{aligned} t.\left(\frac{\alpha}{t'.\alpha.\sigma}\right).\sigma &= t.\left(\frac{\alpha}{\min\left(1, \frac{t.\alpha.\sigma}{t.\underline{1}.\sigma}\right)}\right).\sigma \\ &= t\left(\alpha \sqcup \frac{t.\underline{1}.\sigma \times \alpha}{t.\alpha.\sigma}\right) \\ &\geq t.\underline{1}.\sigma, \end{aligned}$$

and

$$t'.(\frac{\alpha}{t'.\alpha.\sigma}).\sigma = \min\left(1, \frac{t.(\frac{\alpha}{t'.\alpha.\sigma}).\sigma}{t.\underline{1}.\sigma}\right) = 1.$$

In summary, t' fulfils the conditions (1) to (4) in Theorem 21. Thus, there is $R : \Sigma \leftrightarrow \Gamma$ such that $t' = [R]$. Finally, the assumption (2) warrants that

$$t = \{t.\underline{1}\}; [t.\underline{1}]; t = \{t.\underline{1}\}; t' = \{t.\underline{1}\}; [R].\#$$

Comparing the above corollary and Theorem 21, we find that the only difference between them is that the condition (2) in Theorem 21 is removed. The price is that the condition (4) in Theorem 21 has to be replaced by a much complicated one, that is, the condition (3) in Corollary 22. The above theorem and its corollary generalize Theorems 26.2 and 26.4, respectively, in [4].

To conclude this section, we consider continuity of probabilistic predicate transformers.

Definition 11. *Let Σ and Γ be state spaces. Then $t : \Sigma \mapsto \Gamma$ is continuous if for any directed subset $\{\alpha_i \mid i \in I\}$ of $(\mathbf{P}\Gamma, \equiv>)$,*

$$t.(\sqcup i \in I \cdot \alpha_i) \equiv (\sqcup i \in I \cdot t.\alpha_i)$$

whenever $(\sqcup i \in I \cdot \alpha_i)$ exists.

The following proposition shows that continuity can help us to derive a general strong monotonicity from a finite strong monotonicity.

Proposition 23. *Let $t : \Sigma \mapsto \Gamma$ be continuous. If for any $\alpha, \beta : \mathbf{P}\Gamma$ with finite $\{\gamma : \Gamma \mid \alpha.\gamma > 0\}$ and $\{\gamma : \Gamma \mid \beta.\gamma > 0\}$, we have the finite strong monotonicity*

$$\text{(FSM)} \qquad \lceil \alpha \equiv> \beta \rceil \leq \lceil t.\alpha \equiv> t.\beta \rceil,$$

then t is strongly monotone.

Proof. Let $\mathbf{F}\Gamma$ be the set of finite subsets of Γ. For any $\alpha : \mathbf{P}\Gamma$ and $\Delta \in \mathbf{F}\Gamma$ we write $\alpha \mid \Delta$ for the restriction of α on Δ, i.e.,

$$(\alpha \mid \Delta).\gamma = \begin{cases} \alpha.\gamma \text{ if } \gamma \in \Delta, \\ 0 \text{ otherwise.} \end{cases}$$

Then $\{\alpha \mid \Delta \mid \Delta \in \mathbf{F}\Gamma\}$ is a directed subset of $(\mathbf{P}\Gamma, \equiv>)$ and $\alpha = (\sqcup \Delta \in \mathbf{F}\Gamma \cdot \alpha \mid \Delta)$. Furthermore, from the (FSM) and continuity of t we have

$$\begin{aligned} \lceil t.\alpha \equiv> t.\beta \rceil &= \lceil (\sqcup \Delta \in \mathbf{F}\Gamma \cdot t.(\alpha \mid \Delta)) \equiv> (\sqcup \Delta \in \mathbf{F}\Gamma \cdot t.(\beta \mid \Delta)) \rceil \\ &\geq (\sqcap \Delta \in \mathbf{F}\Gamma \cdot \lceil t.(\alpha \mid \Delta) \equiv> t.(\beta \mid \Delta) \rceil) \\ &\geq (\sqcap \Delta \in \mathbf{F}\Gamma \cdot \lceil \alpha \mid \Delta \equiv> \beta \mid \Delta \rceil). \end{aligned}$$

Finally, we only need to note that

$$\lceil \alpha \mid \Delta \equiv> \beta \mid \Delta \rceil \geq \lceil \alpha \equiv> \beta \rceil.\#$$

The following proposition is a probabilistic generalization of Theorem 22.5 in [4] and it presents a necessary and sufficient condition for a demonic update to be continuous.

Proposition 24. *Let $R : \Sigma \leftrightarrow \Gamma$. Then $[R]$ is continuous if and only if for each $\sigma : \Sigma$, $\{\gamma : \Gamma \mid R.\sigma.\gamma > 0\}$ is nonempty and finite.*

Proof. ($\Leftarrow$) Suppose that $\{\alpha_i \mid i \in I\}$ is a directed subset of $(\mathbf{P}\Gamma, \equiv>)$. For any $\sigma : \Sigma$, we want to show that

$$[R].(\sqcup i \in I \cdot \alpha_i).\sigma = (\sqcup i \in I \cdot [R].\alpha_i.\sigma).$$

Note that it suffices to prove

$$[R].(\sqcup i \in I \cdot \alpha_i).\sigma \leq (\sqcup i \in I \cdot [R].\alpha_i.\sigma)$$

because the reverse inequality automatically holds. We write

$$\{\gamma : \Gamma \mid R.\sigma.\gamma > 0\} = \{\gamma_1, ..., \gamma_n\}\ (n \geq 1).$$

Then

$$\begin{aligned}
[R].(\sqcup i \in I.\alpha_i).\sigma &= \left(\sqcap \gamma : \Gamma \cdot \min\left[1, \frac{(\sqcup i \in I \cdot \alpha_i.\gamma)}{R.\sigma.\gamma}\right]\right) \\
&= \left(\sqcap_{i=1}^{n} \min\left[1, \frac{(\sqcup i \in I \cdot \alpha_i.\gamma_j)}{R.\sigma.\gamma_j}\right]\right) \\
&= \left(\sqcap_{i=1}^{n} \left(\sqcup i \in I \cdot \min\left[1, \frac{\alpha_i.\gamma_j}{R.\sigma.\gamma_j}\right]\right)\right) \\
&= \left(\sqcup i_1, ..., i_n \in I \cdot \left(\sqcap_{i=1}^{n} \min\left[1, \frac{\alpha_{i_j}.\gamma_j}{R.\sigma.\gamma_j}\right]\right)\right).
\end{aligned}$$

For any $i_1, ..., i_n \in I$, since $\{\alpha_i \mid i \in I\}$ is directed, there is $i_0 \in I$ such that $\alpha_{i_j} \equiv> \alpha_{i_0}$ for all $j = 1, ..., n$. Thus,

$$\begin{aligned}
\left(\sqcap_{i=1}^{n} \min\left[1, \frac{\alpha_{i_j}.\gamma_j}{R.\sigma.\gamma_j}\right]\right) &\leq \left(\sqcap_{i=1}^{n} \min\left[1, \frac{\alpha_{i_0}.\gamma_j}{R.\sigma.\gamma_j}\right]\right) \\
&= \left(\sqcap \gamma : \Gamma \cdot \min\left[1, \frac{\alpha_{i_0}.\gamma}{R.\sigma.\gamma}\right]\right) \\
&= [R].\alpha_{i_0}.\sigma \\
&\leq (\sqcup i \in I \cdot [R].\alpha_i.\sigma)
\end{aligned}$$

because $i_1, ..., i_n$ may range over the whole index set I.

($\Rightarrow$) If for some $\sigma : \Sigma$, $\{\gamma : \Gamma \mid R.\sigma.\gamma > 0\}$ is infinite, then we may assume that it has a countably infinite subset $\Delta = \{\gamma_0, \gamma_1, \gamma_2, ...\}$. For any non-negative integer i, we set

$$\alpha_i.\gamma = \begin{cases} 0 \text{ if } \gamma \in \{\gamma_{i+1}, \gamma_{i+2}, ...\}, \\ R.\sigma.\gamma \text{ if } \gamma \in \Gamma - \{\gamma_{i+1}, \gamma_{i+2}, ...\}. \end{cases}$$

Then $\{\alpha_i \mid i = 0, 1, 2, ...\}$ is a chain in $(\mathbf{P}\Gamma, \equiv>)$ and for all $\gamma : \Gamma$,

$$(\sqcup_{i=0}^{\infty}\alpha_i).\gamma = R.\sigma.\gamma.$$

Consequently,

$$[R].(\sqcup_{i=0}^{\infty}\alpha_i).\sigma = \left(\sqcap\gamma : \Gamma. \min\left[1, \frac{(\sqcup_{i=0}^{\infty}\alpha_i).\gamma}{R.\sigma.\gamma}\right]\right) = 1.$$

On the other hand, for any non-negative integer i,

$$\begin{aligned} [R].\alpha_i.\sigma &= \left(\sqcap\gamma : \Gamma. \min\left(1, \frac{\alpha_i.\gamma}{R.\sigma.\gamma}\right)\right) \\ &\leq \min\left(1, \frac{\alpha_i.\gamma_{i+1}}{R.\sigma.\gamma_{i+1}}\right) = 0, \end{aligned}$$

and

$$(\sqcup_{i=0}^{\infty}[R].\alpha_i.\sigma) = 0.$$

Therefore,

$$[R].(\sqcup_{i=0}^{\infty}\alpha_i) \neq (\sqcup_{i=0}^{\infty}[R].\alpha_i),$$

and $[R]$ is not continuous.#

Continuity is preserved by parallel composition, angelic choice and finite demonic choice.

Proposition 25. *(1) If t_1 and t_2 are both continuous, so is $t_1; t_2$.*
(2) If t_i $(i \in I)$ are all continuous, so is $(\sqcup i \in I \cdot t_i)$.
(3) If t_1 and t_2 are continuous, so is $t_1 \sqcap t_2$.

Proof. Easy.

We finally establish a normal form theorem for probabilistic continuous predicate transformers. This theorem indicates that a continuous probabilistic predicate transformer can be written as a composition of a probabilistic angelic update and a probabilistic demonic update, and the probabilistic relation used in the demonic update could be chosen to be image-finite. The major difference between the probabilistic case and the usual (Boolean) one is that the condition of finite strong monotonicity has to be imposed. Note that the monotonicity of a Boolean predicate transformer automatically

holds provided it is continuous. However, it is not the case for probabilistic predicate transformers, and the finite strong monotonicity of a probabilistic predicate transformer is not implied by its continuity.

Theorem 26. *Let Σ and Γ be state spaces and $t : \Sigma \mapsto \Gamma$. Then t is continuous and satisfies (FSM) if and only if*

$$t = \{R\}; [R']$$

for some probabilistic relations R and R' with $\phi \neq \{\gamma : \Gamma \mid R'.\lambda.\gamma > 0\}$ is finite for all $\lambda : \Lambda$, where Λ is the domain of R'.

Proof. ($\Leftarrow$) It is obvious from Propositions 18(1), 24 and 25(1).

($\Rightarrow$) We follow the idea used in the proof of Theorem 26.16 in [4]. Let

$$\mathbf{F}_+\Gamma := \{\alpha : \mathbf{P}\Gamma \mid \phi \neq \{\gamma : \Gamma \mid \alpha.\gamma > 0\} \text{ is finite}\},$$

and let $R : \Sigma \leftrightarrow \mathbf{F}_+\Gamma$ and $R' : \mathbf{F}_+\Gamma \leftrightarrow \Gamma$ be defined in the same way as in the proof of Theorem 12, i.e., for any $\sigma : \Sigma$, $\beta : \mathbf{F}_+\Gamma$ and $\gamma : \Gamma$,

$$R.\sigma.\beta := t.\beta.\sigma,$$
$$R'.\beta.\gamma := \beta.\gamma.$$

Then it is easy to see that $\phi \neq \{\gamma : \Gamma \mid R'.\beta.\gamma > 0\}$ is finite for each $\beta : \mathbf{F}_+\Gamma$. With an argument similar to that in the proof of Theorem 12 we are able to prove

$$t.\alpha = (\{R\}; [R']).\alpha$$

for all $\alpha : \mathbf{F}_+\Gamma$ (note that (FSM) is satisfied by t). Finally, for all $\alpha : \mathbf{P}\Gamma$,

$$\begin{aligned} t.\alpha &= (\sqcup \alpha' : \mathbf{F}_+\Gamma \mid \alpha' \equiv> \alpha \cdot t.\alpha') \\ &= (\sqcup \alpha' : \mathbf{F}_+\Gamma \mid \alpha' \equiv> \alpha \cdot (\{R\}; [R']).\alpha') \\ &= (\{R\}; [R']).\alpha, \end{aligned}$$

where the first equality is from the continuity of t (cf. the proof of Proposition 23), and the third one is because $\{R\}$ is universally disjunctive and $[R]$ is continuous (Propositions 18(1) and 24).#

6 Probabilistic refinement and correctness

One of the most important method for program construction is stepwise refinement which was advocated by E. W. Dijkstra [10, 11] and N. Wirth [44] in the early 1970's. This method may help us to derive an executable program from a high-level specification through a process of replacing subspecifications by program statements step by step. As its systematic formalization, R. -J. Back [4] has developed a calculus for refinements. A similar

approach was also proposed by C. C. Morgan [28]. The central notion of their calculus is refinement relation which preserves correctness of programs. In [24, 29], the notion of refinement was already generalized to probabilistic predicate transformers; see also Definition 1(3). It may be noted that probabilistic refinement introduced in [24, 29] is defined in the same way as that of the refinement relation for non-probabilistic predicate transformers where there are only two extreme cases: a probabilistic predicate transformer is refined by another or not, absolutely. We believe that such a refinement relation is over-simplified for probabilistic programs. Indeed, it is still an ordinary (sharp) relation but not probabilistic one in the sense that a probabilistic predicate transformer may be refined by another with a belief probability less than 1. The main reason of having a sharp refinement for probabilistic programs in [24, 29] is that the underlying (meta-)logic used there is classical two-valued logic. By employing a probabilistic logic, we are able to propose a more probabilistic and subtler notion of refinement.

Definition 12. *Let Σ and Γ be two state spaces, and let $t, t' : \Sigma \mapsto \Gamma$. The refinement index of t by t' is defined as*

$$\lceil t \sqsubseteq t' \rceil := (\sqcap \alpha : \mathbf{P}\Gamma \cdot \lceil t.\alpha \equiv> t'.\alpha \rceil).$$

The intuitive meaning of the refinement index $\lceil t \sqsubseteq t' \rceil$ is the belief degree (or probability) of the statement that t is refined by t'. The main idea behind the above definition is that instead of talking about an absolute refinement, we give a belief probability to which a probabilistic predicate transformer is refined by another. The belief probability is given by the truth value of a probabilistic logical translation of the defining statement of classical refinement. Thus, we have a graded notion of refinement, and it provides us with a continuous spectrum of refinement strength for probabilistic programs. At the top of this spectrum is the probabilistic refinement introduced in [24, 29]. To see how our proposed notion of refinement index is used to describe more flexibly certain refinement relation between probabilistic predicate transformers, we examine a simple example. Let $\sigma_0 : \Sigma$, let t' be *skip*, that is, $t'.\alpha = \alpha$ for all $\alpha : \mathbf{P}\Sigma$, and let t be an $\varepsilon-$pulse $abort_{\sigma_0,\varepsilon}$ of $abort$ at σ_0 and

$$abort_{\sigma_0,\varepsilon}.\alpha = \begin{cases} false \text{ if } \alpha \neq \overline{\sigma_0}, \\ (1+\varepsilon) \times \overline{\sigma_0} \text{ if } \alpha = \overline{\sigma_0}. \end{cases}$$

It is clear that $t.\alpha \equiv> t'.\alpha$ for all α except $\overline{\sigma_0}$. $t.\overline{\sigma_0}$ exceeds $t'.\overline{\sigma_0}$, but not too much, and they are almost the same when ε is very small. However, no matter how small ε is, it does not hold that $t \sqsubseteq t'$ according to Definition

1(3). On the other hand, with Definition 12 we have

$$\lceil t \sqsubseteq t' \rceil = \lceil (1+\varepsilon) \times \overline{\sigma_0} \mathrel{=\!\!>} \overline{\sigma_0} \rceil = \frac{1}{1+\varepsilon}.$$

This means that for a small parameter ε, we will have a very high belief probability of refinement between t and t'.

The following proposition shows that the refinement of probabilistic updates is equivalent to the implication relation between the respective probabilistic relations, and probabilistic refinement is preserved by various operations of probabilistic predicate transformers.

Proposition 27. *Let Σ, Γ and Δ be state spaces, $P, Q : \Sigma \leftrightarrow \Gamma$, $t, t', t'', t_1, t_1', t_i\ (i \in I) : \Sigma \mapsto \Gamma$ and $t_2, t_2' : \Gamma \mapsto \Delta$. Then*
(1) $\lceil t \sqsubseteq t' \rceil \times \lceil t' \sqsubseteq t'' \rceil \leq \lceil t \sqsubseteq t'' \rceil$.
(2) $\lceil P \mathrel{=\!\!>} Q \rceil = \lceil \{P\} \sqsubseteq \{Q\} \rceil$.
(3) $\lceil P \mathrel{=\!\!>} Q \rceil = \lceil [Q] \sqsubseteq [P] \rceil$.
(4) $\lceil t_1 \sqsubseteq t_1' \rceil \leq \lceil t_1; t_2 \sqsubseteq t_1'; t_2 \rceil$, *and if t_1 is strongly monotone, then* $\lceil t_2 \sqsubseteq t_2' \rceil \leq \lceil t_1; t_2 \sqsubseteq t_1; t_2' \rceil$.
(5) $(\sqcap i \in I \cdot \lceil t_i \sqsubseteq t_i' \rceil) \leq \lceil (\sqcap i \in I \cdot t_i) \sqsubseteq (\sqcap i \in I \cdot t_i') \rceil$.
(6) $(\sqcap i \in I \cdot \lceil t_i \sqsubseteq t_i' \rceil) \leq \lceil (\sqcup i \in I \cdot t_i) \sqsubseteq (\sqcup i \in I \cdot t_i') \rceil$ *if both* $(\sqcup i \in I . t_i)$ *and* $(\sqcup i \in I \cdot t_i')$ *exist.*

Proof. We only prove (3). (1) is immediate from Definition 12 and Proposition 8(1). (2) is similar to (3), (4) is easy, and (5) and (6) are similar to Proposition 8(5) and (6). First, we have

$$\begin{aligned}\lceil [Q] \sqsubseteq [P] \rceil &= (\sqcap \alpha : \mathbf{P}\Gamma \cdot \lceil [Q].\alpha \mathrel{=\!\!>} [P].\alpha \rceil) \\ &= \left(\sqcap \alpha : \mathbf{P}\Gamma \cdot \sigma : \Sigma . \min \left[1, \frac{[P].\alpha.\sigma}{[Q].\alpha.\sigma} \right] \right).\end{aligned}$$

For any $\alpha : \mathbf{P}\Gamma$ and $\sigma : \Sigma$, it holds that

$$\begin{aligned}\frac{[P].\alpha.\sigma}{[Q].\alpha.\sigma} &= \frac{\left(\sqcap \gamma : \Gamma \cdot \min \left(1, \frac{\alpha.\gamma}{P.\sigma.\gamma} \right) \right)}{\left(\sqcap \gamma : \Gamma \cdot \min \left(1, \frac{\alpha.\gamma}{Q.\sigma.\gamma} \right) \right)} \\ &= \left(\sqcap \gamma : \Gamma \cdot \frac{\min \left(1, \frac{\alpha.\gamma}{P.\sigma.\gamma} \right)}{\left(\sqcap \gamma' : \Gamma \cdot \min \left(1, \frac{\alpha.\gamma'}{Q.\sigma.\gamma'} \right) \right)} \right) \\ &\geq \left(\sqcap \gamma : \Gamma \cdot \frac{\min(1, \frac{\alpha.\gamma}{P.\sigma.\gamma})}{\min \left(1, \frac{\alpha.\gamma}{Q.\sigma.\gamma} \right)} \right) \\ &= \left(\sqcap \gamma : \Gamma \cdot \min \left[\frac{1}{\min(1, \frac{\alpha.\gamma}{Q.\sigma.\gamma})}, \frac{\frac{\alpha.\gamma}{P.\sigma.\gamma}}{\min \left(1, \frac{\alpha.\gamma}{Q.\sigma.\gamma} \right)} \right] \right)\end{aligned}$$

$$\begin{aligned}
&\geq \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{\alpha.\gamma}{\frac{P.\sigma.\gamma}{\alpha.\gamma}}\right)\right) \\
&= \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{Q.\sigma.\gamma}{P.\sigma.\gamma}\right)\right) \\
&\geq \left(\sqcap\sigma' : \Sigma \cdot \gamma : \Gamma \cdot \min\left(1, \frac{Q.\sigma'.\gamma}{P.\sigma'.\gamma}\right)\right) \\
&= \lceil P \equiv\!> Q \rceil.
\end{aligned}$$

This leads to $\lceil P \equiv\!> Q \rceil \leq \lceil [Q] \sqsubseteq [P] \rceil$.

On the other hand, knowing that P and Q are bounded, we are able to find $M \in \mathbf{R}_{\geq}$ such that $P.\sigma.\gamma \leq M$ and $Q.\sigma.\gamma \leq M$ for all $\sigma : \Sigma$ and $\gamma : \Gamma$. Now for any $\sigma : \Sigma$ and $\gamma' : \Gamma$, we define $\alpha_0 : \mathbf{P}\Gamma$ by

$$\alpha_0.\gamma = \begin{cases} Q.\sigma.\gamma' & \text{if } \gamma = \gamma', \\ M & \text{if } \gamma \in \Gamma - \{\gamma'\}. \end{cases}$$

Then by a routine calculation we obtain

$$[P].\alpha_0.\sigma = \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{\alpha_0.\gamma}{P.\sigma.\gamma}\right)\right) = \min\left(1, \frac{Q.\sigma.\gamma'}{P.\sigma.\gamma}\right),$$

and

$$[Q].\alpha_0.\sigma = \left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{\alpha_0.\gamma}{Q.\sigma.\gamma}\right)\right) = 1.$$

Therefore,

$$\begin{aligned}
\lceil [Q] \sqsubseteq [P] \rceil &\leq \frac{[P].\alpha_0.\sigma}{[Q].\alpha_0.\sigma} \\
&= \min\left(1, \frac{Q.\sigma.\gamma'}{P.\sigma.\gamma}\right).
\end{aligned}$$

From arbitrariness of σ and γ', it follows that

$$\begin{aligned}
\lceil [Q] \sqsubseteq [P] \rceil &\leq \left(\sqcap\sigma : \Sigma \cdot \gamma' : \Gamma \cdot \min\left(1, \frac{Q.\sigma.\gamma'}{P.\sigma.\gamma}\right)\right) \\
&= \lceil P \equiv\!> Q \rceil.\#
\end{aligned}$$

The above proof can be rewritten in a much more elegant form by exploiting the power of the Galois connection given after Definition 7. We first notice that for any $x \in [0,1]$, $\alpha : \mathbf{P}\Sigma$ and $\sigma : \Sigma$,

$$x \leq \alpha.\sigma \text{ if and only if } x \times \lceil \alpha \equiv\!> \beta \rceil \leq \beta.\sigma \text{ for all } \beta : \mathbf{P}\Sigma.$$

Then for all $x \in [0,1]$,

$$x \leq \lceil [Q] \sqsubseteq [P] \rceil$$

iff (Definition 12)

$$x \leq \lceil [Q].\alpha \mathrel{=\!\!>} [P].\alpha \rceil \text{ for all } \alpha$$

iff (the Galois connection after Definition 7)

$$x \times [Q].\alpha.\gamma \leq [P].\alpha.\gamma \text{ for all } \alpha, \gamma$$

iff (the remark after Definition 6)

$$x \times \lceil Q_\Sigma.\gamma \mathrel{=\!\!>} \alpha \rceil \leq \lceil P_\Sigma.\gamma \mathrel{=\!\!>} \alpha \rceil \text{ for all } \alpha, \gamma$$

iff (the Galois connection after Definition 7)

$$x \times \lceil Q_\Sigma.\gamma \mathrel{=\!\!>} \alpha \rceil \times P.\sigma.\gamma \leq \alpha.\sigma \text{ for all } \alpha, \sigma, \gamma$$

iff

$$(\text{for all } \alpha,\ x \times P.\sigma.\gamma \times \lceil Q_\Sigma.\gamma \mathrel{=\!\!>} \alpha \rceil \leq \alpha.\sigma) \text{ for all } \sigma, \gamma$$

iff (the claim at the beginning of this proof)

$$x \times P.\sigma.\gamma \leq Q.\sigma.\gamma$$

iff (the Galois connection after Definition 7)

$$x \leq \lceil P \mathrel{=\!\!>} Q \rceil.$$

Since x was arbitrary, the desired inequality follows. The idea behind this proof could also apply to give simpler proofs of some other results.

The following proposition evaluates the probabilistic refinement strength between some specification statements.

Proposition 28. *(1)* $\lceil P \mathrel{=\!\!>} P' \rceil \times \lceil Q \mathrel{=\!\!>} Q' \rceil \leq \lceil \{P\}; [Q] \sqsubseteq \{P'\}; [Q'] \rceil$.
(2) $\lceil p \mathrel{=\!\!>} p' \rceil \times \lceil Q' \mathrel{=\!\!>} Q \rceil \leq \lceil \{p\}; [Q] \sqsubseteq \{p'\}; [Q'] \rceil \leq \min\left(\lceil p \mathrel{=\!\!>} p' \rceil, \frac{\lceil Q' \mathrel{=\!\!>} Q \rceil}{\lceil p' \mathrel{=\!\!>} p \rceil} \right)$.
(3) $\lceil |\ p\ | \times Q' \mathrel{=\!\!>} |\ p'\ | \times Q \rceil \leq \lceil [p]; \{Q\} \sqsubseteq [p']; \{Q'\} \rceil$

$$\leq \lceil p \times dom.Q' \mathrel{=\!\!>} p' \times dom.Q \rceil,$$

where the second inequality is subject to the condition that there exists γ *with* $Q.\sigma.\gamma > 0$ *for all* σ.
(4) $\lceil \{P\}; [Q] \sqsubseteq \{p'\}; [Q'] \rceil = \min(\lceil dom.P \mathrel{=\!\!>} p' \rceil,$

$$\lceil |\ P\ | \times |\ Q'\ | \mathrel{=\!\!>} |\ p'\ | \times |\ Q\ | \rceil),$$

where we suppose that $P : \Sigma \leftrightarrow \Gamma, Q : \Gamma \leftrightarrow \Delta, p' : \mathbf{P}\Sigma$ *and* $Q : \Sigma \leftrightarrow \Delta$, *and* $|\ P\ |, |\ Q\ |, |\ p'\ |, |\ Q'\ |$ *are the cylindric extensions of* P, Q, p' *and* Q', *respectively, on the product type* $\Sigma \times \Gamma \times \Delta$, *i.e., for any* $\sigma : \Sigma, \gamma : \Gamma$ *and* $\delta : \Delta$,

$$|\ P\ |.\sigma.\gamma.\delta := P.\sigma.\gamma, \qquad |\ Q\ |.\sigma.\gamma.\delta := Q.\gamma.\delta,$$

$$| p' | .\sigma.\gamma.\delta := p'.\sigma \qquad | Q' | .\sigma.\gamma.\delta := Q'.\sigma.\delta.$$

(5) $\lceil \{P\}; [Q] \sqsubseteq [p']; \{Q'\} \rceil = \min(\lceil dom.P \equiv> \underline{1} \rceil, \lceil | p' | \times P \equiv> Q' \circ Q^{-1} \rceil)$.

Proof. (1) It is immediate from Propositions 12(1) to (4).
(2) For simplicity, we write λ for $\lceil \{p\}; [Q] \sqsubseteq \{p'\}; [Q'] \rceil$. First, by a simple calculation we have for any α, σ

$$(\{p\}; [Q]).\alpha.\sigma = p.\sigma \times \lceil Q.\sigma \equiv> \alpha \rceil,$$

where $Q.\sigma$ is a probabilistic predicate and $(Q.\sigma).\gamma := Q.\sigma.\gamma$ for all γ. Therefore,

$$\begin{aligned}
\lambda &= (\sqcap\alpha \cdot \lceil (\{p\}; [Q]).\alpha \equiv> (\{p'\}; [Q']).\alpha \rceil. \\
&= \left(\sqcap\alpha, \sigma \cdot \min \left[1, \frac{(\{p'\}; [Q']).\alpha.\sigma}{(\{p\}; [Q]).\alpha.\sigma} \right] \right) \\
&= \left(\sqcap\alpha, \sigma \cdot \min \left(1, \frac{p'.\sigma \times \lceil Q'.\sigma \equiv> \alpha \rceil}{p.\sigma \times \lceil Q.\sigma \equiv> \alpha \rceil} \right) \right) \\
&\leq \left(\sqcap\sigma \cdot \min \left(1, \frac{p'.\sigma \times \lceil Q'.\sigma \equiv> Q.\sigma \rceil}{p.\sigma \times \lceil Q.\sigma \equiv> Q.\sigma \rceil} \right) \right) \\
&= \left(\sqcap\sigma \cdot \min \left(1, \frac{p'.\sigma}{p.\sigma} \times \lceil Q'.\sigma \equiv> Q.\sigma \rceil \right) \right).
\end{aligned}$$

Conversely, note that

$$\lceil Q'.\sigma \equiv> \alpha \rceil \geq \lceil Q'.\sigma \equiv> Q.\sigma \rceil \times \lceil Q.\sigma \equiv> \alpha \rceil.$$

Thus,

$$\begin{aligned}
\lambda &\geq \left(\sqcap\alpha, \sigma \cdot \min \left(1, \frac{p'.\sigma \times \lceil Q'.\sigma \equiv> Q.\sigma \rceil \times \lceil Q.\sigma \equiv> \alpha \rceil}{p.\sigma \times \lceil Q.\sigma \equiv> \alpha \rceil} \right) \right) \\
&= \left(\sqcap\sigma \cdot \min \left(1, \frac{p'.\sigma}{p.\sigma} \times \lceil Q'.\sigma \equiv> Q.\sigma \rceil \right) \right).
\end{aligned}$$

By combining the above inequalities we obtain

$$\lambda = \left(\sqcap\sigma \cdot \min \left(1, \frac{p'.\sigma}{p.\sigma} \times \lceil Q'.\sigma \equiv> Q.\sigma \rceil \right) \right).$$

From the definition of $Q.\sigma$, it is easy to see that for any σ,

$$\lceil Q'.\sigma \equiv> Q.\sigma \rceil \geq (\sqcap\sigma'.\lceil Q'.\sigma' \equiv> Q.\sigma' \rceil) = \lceil Q' \equiv> Q \rceil.$$

Then it follows that

$$\begin{aligned}\lambda &\geq \left(\sqcap\sigma \cdot \min\left(1, \frac{p'.\sigma}{p.\sigma} \times \lceil Q' \equiv> Q\rceil\right)\right)\\ &\geq \left(\sqcap\sigma \cdot \min\left(1, \frac{p'.\sigma}{p.\sigma}\right)\right) \times \lceil Q' \equiv> Q\rceil\\ &= \lceil p \equiv> p'\rceil \times \lceil Q' \equiv> Q\rceil.\end{aligned}$$

On the other hand, since it always holds that $\lceil Q'.\sigma \equiv> Q.\sigma\rceil \leq 1$, we have

$$\lambda \geq \left(\sqcap\sigma \cdot \min\left(1, \frac{p'.\sigma}{p.\sigma}\right)\right) = \lceil p \equiv> p'\rceil.$$

Moreover, we can see that for all σ,

$$\lambda \leq \frac{p'.\sigma}{p.\sigma} \times \lceil Q'.\sigma \equiv> Q.\sigma\rceil$$

from the above conclusion, and

$$\lambda \times \min\left(1, \frac{p.\sigma}{p'.\sigma}\right) \leq \lambda \times \frac{p.\sigma}{p'.\sigma} \leq \lceil Q'.\sigma \equiv> Q.\sigma\rceil.$$

Consequently,

$$\begin{aligned}\lambda \times \lceil p' \equiv> p\rceil &= \left(\sqcap\sigma \cdot \lambda \times \min\left(1, \frac{p.\sigma}{p'.\sigma}\right)\right)\\ &\leq (\sqcap\sigma \cdot \lceil Q'.\sigma \equiv> Q.\sigma\rceil)\\ &= \lceil Q' \equiv> Q\rceil,\end{aligned}$$

and

$$\lambda \leq \frac{\lceil Q' \equiv> Q\rceil}{\lceil p' \equiv> p\rceil}.$$

(3) For any α and σ, we have

$$([p]; \{Q\}).\alpha.\sigma = \min\left(1, \frac{\{Q\}.\alpha.\sigma}{p.\sigma}\right).$$

By a routine calculation we can obtain

$$\begin{aligned}&\lceil [p]; \{Q\} \sqsubseteq [p']; \{Q'\}\rceil\\ &= \left(\sqcap\alpha, \sigma \cdot \min\left(1, \frac{p.\sigma}{\{Q\}.\alpha.\sigma}\right) \sqcup \min\left(1, \frac{p.\sigma}{p'.\sigma} \times \frac{\{Q'\}.\alpha.\sigma}{\{Q\}.\alpha.\sigma}\right)\right)\\ &\geq \left(\sqcap\alpha, \sigma \cdot \min\left(1, \frac{p.\sigma}{p'.\sigma} \times \frac{\{Q'\}.\alpha.\sigma}{\{Q\}.\alpha.\sigma}\right)\right)\\ &\geq \left(\sqcap\sigma \cdot \min\left[1, \frac{p.\sigma}{p'.\sigma} \times \left(\sqcap\gamma \cdot \frac{Q'.\sigma.\gamma}{Q.\sigma.\gamma}\right)\right]\right)\end{aligned}$$

$$= \left(\sqcap\sigma, \gamma \cdot \min\left(1, \frac{p.\sigma}{p'.\sigma} \times \frac{Q'.\sigma.\gamma}{Q.\sigma.\gamma}\right)\right)$$
$$= \lceil\!| \, p \mid \times Q' \equiv\!>\!| \, p' \mid \times Q \, |\!\rceil.$$

We now turn to prove the second inequality. For any $a : \mathbf{R}_{\geq}$ and $\sigma : \Sigma$, it is easy to know that $\{Q\}.\underline{a}.\sigma = a \times dom.Q.\sigma$. Then

$$\begin{aligned}
&\lceil [p]; \{Q\} \sqsubseteq [p']; \{Q'\} \rceil \\
&\leq \left(\sqcap\sigma \cdot \min\left(1, \frac{p.\sigma}{\{Q\}.\underline{a}.\sigma}\right) \sqcup \min\left(1, \frac{p.\sigma}{p'.\sigma} \times \frac{\{Q'\}.\underline{a}.\sigma}{\{Q\}.\underline{a}.\sigma}\right)\right) \\
&= \left(\sqcap\sigma \cdot \min\left(1, \frac{p.\sigma}{a \times dom.Q.\sigma}\right) \sqcup \min\left(1, \frac{p.\sigma}{p'.\sigma} \times \frac{a \times dom.Q'.\sigma}{a \times dom.Q.\sigma}\right)\right) \\
&= \left(\sqcap\sigma \cdot \min\left(1, \frac{p.\sigma}{a \times dom.Q.\sigma}\right) \sqcup \min\left(1, \frac{p.\sigma}{p'.\sigma} \times \frac{dom.Q'.\sigma}{dom.Q.\sigma}\right)\right).
\end{aligned}$$

It follows that $dom.Q.\sigma > 0$ from the condition: it holds that $Q.\sigma.\gamma > 0$ for some γ. Let $a \to \infty$. We obtain

$$\begin{aligned}
\lceil [p]; \{Q\} \sqsubseteq [p']; \{Q'\} \rceil &\leq \left(\sqcap\sigma \cdot \min\left(1, \frac{p.\sigma}{p'.\sigma} \times \frac{dom.Q'.\sigma}{dom.Q.\sigma}\right)\right) \\
&\leq \lceil p \times dom.Q' \equiv\!> p' \times dom.Q \rceil.
\end{aligned}$$

(4) With a reasoning similar to that in the proof of (2), we can obtain

$$\begin{aligned}
&\lceil \{P\}; [Q] \sqsubseteq \{p'\}; [Q'] \rceil = \left(\sqcap\sigma, \gamma \cdot \min\left(1, \frac{p'.\sigma}{P.\sigma.\gamma} \times \lceil Q'.\sigma \equiv\!> Q.\gamma \rceil\right)\right) \\
&= \left(\sqcap\sigma, \gamma \cdot \min\left[1, \frac{p'.\sigma}{P.\sigma.\gamma} \times \left(\sqcap\delta \cdot \min\left(1, \frac{Q.\gamma.\delta}{Q'.\sigma.\gamma}\right)\right)\right]\right) \\
&= \left(\sqcap\sigma, \gamma, \delta \cdot \min\left[1, \min\left(\frac{p'.\sigma}{P.\sigma.\gamma}, \frac{p'.\sigma}{P.\sigma.\gamma} \times \frac{Q.\gamma.\delta}{Q'.\sigma.\gamma}\right)\right]\right) \\
&= \left(\sqcap\sigma, \gamma \cdot \min\left(1, \frac{p'.\sigma}{P.\sigma.\gamma}\right)\right) \sqcap \left(\sqcap\sigma, \gamma, \delta \cdot \min\left(1, \frac{p'.\sigma}{P.\sigma.\gamma} \times \frac{Q.\gamma.\delta}{Q'.\sigma.\gamma}\right)\right) \\
&= \left(\sqcap\sigma \cdot \min\left(1, \frac{p'.\sigma}{(\sqcup\gamma \cdot P.\sigma.\gamma)}\right)\right) \sqcap \lceil\!| \, P \mid \times \mid Q' \mid\equiv\!>\!| \, p' \mid \times \mid Q \mid \rceil \\
&= \min\left(\lceil dom.P \equiv\!> p' \rceil, \lceil\!| \, P \mid \times \mid Q' \mid\equiv\!>\!| \, p' \mid \times \mid Q \mid \rceil\right).
\end{aligned}$$

(5) A routine calculation yields

$$\begin{aligned}
&\lceil \{P\}; [Q] \sqsubseteq [p']; \{Q'\} \rceil \\
&= \left(\sqcap\alpha,\sigma,\gamma \cdot \min\left[1, \frac{1}{P.\sigma.\gamma \times \lceil Q.\gamma \equiv\!> \alpha \rceil}, \frac{\{Q'\}.\alpha.\sigma}{p'.\sigma \times P.\sigma.\gamma \times \lceil Q.\gamma \equiv\!> \alpha \rceil}\right]\right) \\
&= \left(\sqcap\alpha,\sigma,\gamma \cdot \min\left(1, \frac{1}{P.\sigma.\gamma \times \lceil Q.\gamma \equiv\!> \alpha \rceil}\right)\right)
\end{aligned}$$

$$\sqcap\left(\sqcap\alpha,\sigma,\gamma\cdot\min\left(1,\frac{\{Q'\}.\alpha.\sigma}{p'.\sigma\times P.\sigma.\gamma\times\lceil Q.\gamma\equiv>\alpha\rceil}\right)\right).$$

We now note that

$$\begin{aligned}&\left(\sqcap\alpha,\sigma,\gamma\cdot\min\left(1,\frac{1}{P.\sigma.\gamma\times\lceil Q.\gamma\equiv>\alpha\rceil}\right)\right)\\&=\left(\sqcap\sigma,\gamma\cdot\min\left(1,\frac{1}{P.\sigma.\gamma}\right)\right)\\&=\left(\sqcap\sigma\cdot\min\left(1,\frac{1}{dom.P.\sigma}\right)\right)\\&=\lceil dom.P\equiv>\underline{1}\rceil.\end{aligned}$$

Additionally, we have

$$\begin{aligned}\frac{\{Q'\}.\alpha.\sigma}{\lceil Q.\gamma\equiv>\alpha\rceil}&=\frac{(\sqcup\delta\cdot Q'.\sigma.\delta\times\alpha.\delta)}{\lceil Q.\gamma\equiv>\alpha\rceil}\\&=\left(\sqcup\delta\cdot\frac{Q'.\sigma.\delta\times\alpha.\delta}{\lceil Q.\gamma\equiv>\alpha\rceil}\right)\\&=\left(\sqcup\delta\cdot\frac{Q'.\sigma.\delta\times\alpha.\delta}{\left(\sqcap\delta'\cdot\min\left(1,\frac{\alpha.\delta'}{Q.\gamma.\delta'}\right)\right)}\right)\\&\geq\left(\sqcup\delta\cdot\frac{Q'.\sigma.\delta\times\alpha.\delta}{\frac{\alpha.\delta}{Q.\gamma.\delta}}\right)\\&=(\sqcup\delta\cdot Q'.\sigma.\delta\times Q.\delta.\gamma)\\&=(Q'\circ Q^{-1}).\sigma.\gamma.\end{aligned}$$

So, it follows that

$$\begin{aligned}&\left(\sqcap\alpha,\sigma,\gamma\cdot\min\left(1,\frac{\{Q'\}.\alpha.\sigma}{p'.\sigma\times P.\sigma.\gamma\times\lceil Q.\gamma\equiv>\alpha\rceil}\right)\right)\\&\geq\left(\sqcap\sigma,\gamma\cdot\min\left(1,\frac{(Q'\circ Q^{-1}).\sigma.\gamma}{p'.\sigma\times P.\sigma.\gamma}\right)\right)\\&=\lceil|\,p'\mid\times P\equiv>Q'\circ Q^{-1}\rceil).\end{aligned}$$

On the other hand, we have

$$\begin{aligned}&\left(\sqcap\alpha,\sigma,\gamma\cdot\min\left(1,\frac{\{Q'\}.\alpha.\sigma}{p'.\sigma\times P.\sigma.\gamma\times\lceil Q.\gamma\equiv>\alpha\rceil}\right)\right)\\&\leq\left(\sqcap\sigma,\gamma\cdot\min\left(1,\frac{\{Q'\}.(Q.\gamma).\sigma}{p'.\sigma\times P.\sigma.\gamma\times\lceil Q.\gamma\equiv>Q.\gamma\rceil}\right)\right)\\&=\left(\sqcap\sigma,\gamma\cdot\min\left(1,\frac{\{Q'\}.(Q.\gamma).\sigma}{p'.\sigma\times P.\sigma.\gamma}\right)\right)\\&=\lceil|\,p'\mid\times P\equiv>Q'\circ Q^{-1}\rceil).\end{aligned}$$

Thus, we complete the proof by combining the above conclusions.#

It is worthy to note that the role of boundedness of probabilistic relations P and Q is essential in the proof of the above proposition.

A major concept in E. W. Dijkstra's weakest precondition formalization is correctness of a program with respect to a precondition and a postcondition. It may be simply generalized to the probabilistic setting in the following way: a probabilistic predicate transformer t from state space Σ to Γ is correct with respect to a probabilistic predicate α in Σ and β in Γ if and only if $\alpha \equiv> t.\beta$. This is again a highly simplified treatment of probabilistic correctness, and in a sense it only provides a certain qualitative information about correctness of probabilistic programs. In practice such a qualitative description is often restrictive and not sufficient, and we are interested in a quantitative version of correctness of probabilistic programs.

Definition 13. *Let Σ and Γ be two state spaces, $t : \Sigma \mapsto \Gamma$, $\alpha : \mathbf{P}\Sigma$ and $\beta : \mathbf{P}\Gamma$. The correctness index of t with respect to precondition α and postcondition β is defined to be*

$$\lceil \alpha\{|\ t\ |\}\beta \rceil := \lceil \alpha \equiv> t.\beta \rceil.$$

The above definition affords highly flexible machinery for treating correctness of probabilistic programs. Intuitively, $\lceil \alpha\{|\ t\ |\}\beta \rceil$ indicates the belief probability that t is correct with respect to α and β. To be more explicit, let us consider the following example. Let $\sigma_0 : \Sigma$ and t be $skip$, i.e., $t.\alpha = \alpha$ for all $\alpha : \mathbf{P}\Sigma$. If $\alpha = \overline{\sigma_0}$ and $\beta = (1-\varepsilon) \times \overline{\sigma_0}$ is an $\varepsilon-$fluctuation of α, then

$$\lceil \alpha\{|\ t\ |\}\beta \rceil = \lceil \overline{\sigma_0} \equiv> (1-\varepsilon) \times \overline{\sigma_0} \rceil = 1 - \varepsilon.$$

The above equality should be understood that the belief probability of correctness of $skip$ with respect to α and its $\varepsilon-$ fluctuation β is $1-\varepsilon$, and it will converge to 1 as the fluctuation parameter ε approximates 0. This reflects the fact that α and β are almost the same for very small ε.

The idea of approximate correctness was envisaged by the author in [46, 47], and it has been extensively studied in the framework of R. Milner's calculus of communication systems [27] adopting mathematical tools from point-set topology. Further in [48], the author extended his approach to cover probabilistic processes but with a probabilistic logical interpretation as what is done in this paper. A similar idea for probabilistic transition systems was also proposed by F. van Breugel and J. Worrell in [41, 42] where they used a topological device of pseudo-metric too.

The notion of probabilistic refinement may be completely described in terms of probabilistic correctness. This is shown by the next proposition.

Noting that the right-hand side of its conclusion is just the truth value of the statement that for all precondition α and postcondition β, if t is correct with respect α and β, so is t', we know the following proposition means that refinement preserves correctness.

Proposition 29. *Let Σ and Γ be state spaces, and $t, t' : \Sigma \mapsto \Gamma$. Then*

$$\lceil t \sqsubseteq t' \rceil = \left(\sqcap \alpha : \mathbf{P}\Sigma . \beta : \mathbf{P}\Gamma \cdot \min \left[1, \frac{\lceil \alpha \{\mid t' \mid\} \beta \rceil}{\lceil \alpha \{\mid t \mid\} \beta \rceil} \right] \right).$$

Proof. First, note that $\lceil t.\beta \{\mid t \mid\} \beta \rceil = \lceil t.\beta \equiv\!> t.\beta \rceil = 1$. We have

$$\begin{aligned} \text{the right} - \text{hand side} &\leq \left(\sqcap \beta : \mathbf{P}\Gamma \cdot \min \left[1, \frac{\lceil t.\beta \{\mid t' \mid\} \beta \rceil}{\lceil t.\beta \{\mid t \mid\} \beta \rceil} \right] \right) \\ &= (\sqcap \beta : \mathbf{P}\Gamma \cdot \lceil t.\beta \{\mid t' \mid\} \beta \rceil) \\ &= (\sqcap \beta : \mathbf{P}\Gamma \cdot \lceil t.\beta \equiv\!> t'.\beta \rceil) \\ &= \lceil t \sqsubseteq t' \rceil. \end{aligned}$$

Conversely, for any $\alpha : \mathbf{P}\Sigma$ and $\beta : \mathbf{P}\Gamma$, it follows that

$$\begin{aligned} \lceil t \sqsubseteq t' \rceil \times \lceil \alpha \{\mid t \mid\} \beta \rceil &= (\sqcap \beta' : \mathbf{P}\Gamma \cdot \lceil t.\beta' \equiv\!> t'.\beta' \rceil) \times \lceil \alpha \equiv\!> t.\beta \rceil \\ &\leq \lceil t.\beta \equiv\!> t'.\beta \rceil \times \lceil \alpha \equiv\!> t.\beta \rceil \\ &\leq \lceil \alpha \equiv\!> t'.\beta \rceil, \end{aligned}$$

where the last inequality is derived with Proposition 8(1). Consequently, we obtain

$$\lceil t \sqsubseteq t' \rceil \leq \frac{\lceil \alpha \equiv\!> t'.\beta \rceil}{\lceil \alpha \{\mid t \mid\} \beta \rceil} = \frac{\lceil \alpha \{\mid t' \mid\} \beta \rceil}{\lceil \alpha \{\mid t \mid\} \beta \rceil}.$$

Since it always holds that $\lceil t \sqsubseteq t' \rceil \leq 1$, we have

$$\lceil t \sqsubseteq t' \rceil \leq \min \left[1, \frac{\lceil \alpha \{\mid t' \mid\} \beta \rceil}{\lceil \alpha \{\mid t \mid\} \beta \rceil} \right].$$

Finally, arbitrariness of α and β leads to $\lceil t \sqsubseteq t' \rceil \leq$ the right-hand side, and completes the proof.#

A probabilistic predicate transformer is correct with respect to a pair of precondition and postcondition if and only if the corresponding pre-post specification is refined by the probabilistic predicate transformer, and so probabilistic correctness can also be expressed in terms of probabilistic refinement provided the probabilistic predicate transformer under consideration is strongly monotone.

Proposition 30. *Let Σ and Γ be state spaces, $\alpha : \mathbf{P}\Sigma$, $\beta : \mathbf{P}\Gamma$ and $t : \Sigma \mapsto \Gamma$. Then*

$$\lceil \alpha \{\mid t \mid\} \beta \rceil \geq \lceil \{\alpha\}; [\widehat{\beta}] \sqsubseteq t \rceil,$$

and the equality holds if t is strongly monotone, where probabilistic predicate α in the angelic update $\{\alpha\}$ is seen as a probabilistic relation and

$$\alpha.\sigma.\gamma = \begin{cases} \alpha.\sigma \text{ if } \alpha = \gamma, \\ 0 \text{ otherwise}, \end{cases}$$

and $\widehat{\beta}$ is the cylindric extension of β, i.e., a probabilistic relation defined by $\widehat{\beta}.\sigma.\gamma = \beta.\gamma$ for all $\sigma : \Sigma$ and $\gamma : \Gamma$.

Proof. First, we have for any $\sigma : \Sigma$ and $\theta : \mathbf{P}\Gamma$,

$$\begin{aligned} (\{\alpha\}; [\widehat{\beta}]).\theta.\sigma &= \{\alpha\}.([\widehat{\beta}].\theta).\sigma \\ &= \alpha.\sigma \times [\widehat{\beta}].\theta.\sigma \\ &= \alpha.\sigma \times \left(\sqcap \gamma : \Gamma \cdot \min \left[1, \frac{\theta.\gamma}{\widehat{\beta}.\sigma.\gamma} \right] \right) \\ &= \alpha.\sigma \times \left(\sqcap \gamma : \Gamma \cdot \min \left(1, \frac{\theta.\gamma}{\beta.\gamma} \right) \right) \\ &= \alpha.\sigma \times \lceil \beta \equiv> \theta \rceil. \end{aligned}$$

Therefore, it follows that

$$\begin{aligned} \lceil \{\alpha\}; [\widehat{\beta}] \sqsubseteq t \rceil &= (\sqcap \theta : \mathbf{P}\Gamma \cdot \lceil (\{\alpha\}; [\widehat{\beta}]).\theta \equiv> t.\theta \rceil) \\ &\leq \lceil (\{\alpha\}; [\widehat{\beta}]).\beta \equiv> t.\beta \rceil \\ &= \left(\sqcap \sigma : \Sigma \cdot \min \left[1, \frac{t.\beta.\sigma}{(\{\alpha\}; [\widehat{\beta}]).\beta.\sigma} \right] \right) \\ &= \left(\sqcap \sigma : \Sigma \cdot \min \left[1, \frac{t.\beta.\sigma}{\alpha.\sigma \times \lceil \beta \equiv> \beta \rceil} \right] \right) \\ &= \left(\sqcap \sigma : \Sigma \cdot \min \left(1, \frac{t.\beta.\sigma}{\alpha.\sigma} \right) \right) \\ &= \lceil \alpha \equiv> t.\beta \rceil \\ &= \lceil \alpha \{\mid t \mid\} \beta \rceil. \end{aligned}$$

Suppose that t is strongly monotone. Then for any $\theta : \mathbf{P}\Gamma$ and $\sigma : \Sigma$,

$$\begin{aligned} \frac{t.\theta.\sigma}{t.\beta.\sigma} &\geq \left(\sqcap \sigma' : \Sigma \cdot \min \left(1, \frac{t.\theta.\sigma'}{t.\beta.\sigma'} \right) \right) \\ &= \lceil t.\beta \equiv> t.\theta \rceil \\ &\geq \lceil \beta \equiv> \theta \rceil, \end{aligned}$$

where the last inequality is exactly the strong monotonicity of t. Furthermore, it follows that

$$\frac{t.\theta.\sigma}{\alpha.\sigma \times \lceil \beta \equiv> \theta \rceil} \geq \frac{t.\beta.\sigma}{\alpha.\sigma},$$

and

$$\begin{aligned}\lceil\{\alpha\};[\widehat{\beta}]\sqsubseteq t\rceil &= \left(\sqcap\theta:\mathbf{P}\Gamma\cdot\sigma:\Sigma\cdot\min\left[1,\frac{t.\theta.\sigma}{(\{\alpha\};[\widehat{\beta}]).\theta.\sigma}\right]\right)\\ &= \left(\sqcap\theta:\mathbf{P}\Gamma\cdot\sigma:\Sigma\cdot\min\left[1,\frac{t.\theta.\sigma}{\alpha.\sigma\times\lceil\beta\equiv>\theta\rceil}\right]\right)\\ &\geq \left(\sqcap\sigma:\Sigma\cdot\min\left(1,\frac{t.\beta.\sigma}{\alpha.\sigma}\right)\right)\\ &= \lceil\alpha\{|\ t\ |\}\beta\rceil.\#\end{aligned}$$

Correctness of probabilistic update statements may be represented as certain properties of the respective probabilistic relations; and correctness of sequential composition, angelic and demonic choices may be decomposed into correctness of their components. This may be seen from the following rules for probabilistic correctness.

Proposition 31. *Let Σ,Γ and Δ be state spaces, let $\alpha:\mathbf{P}\Sigma$, $\beta:\mathbf{P}\Gamma$, $\theta:\mathbf{P}\Delta$ and $R:\Sigma\leftrightarrow\Gamma$, and let S_1, S_i $(i\in I):\Sigma\mapsto\Gamma$ and $S_2:\Gamma\mapsto\Delta$. Then*
(1) $\lceil\alpha\{|\ \{R\}\ |\}\beta\rceil=(\sqcup f:\Sigma\to\Gamma\cdot\lceil\alpha\equiv>(R;f)\times(\beta;f)\rceil$, where $R;f:\mathbf{P}\Sigma$ is defined by

$$(R;f).\sigma:=R.\sigma.(f.\sigma)$$

for every $\sigma:\Sigma$.
(2) $\lceil\alpha\{|\ [R]\ |\}\beta\rceil=\lceil ran.(|\ \alpha\ |;R)\equiv>\beta\rceil$ if $\alpha.\sigma\leq 1$ for all $\sigma:\Sigma$.
(3) $\lceil\alpha\{|\ S_1;S_2\ |\}\theta\rceil=(\sqcup\beta:\mathbf{P}\Gamma\cdot\lceil\alpha\{|\ S_1\ |\}\beta\rceil\times\lceil\beta\{|\ S_2\ |\}\theta\rceil)$ if S_1 is strongly monotone.
(4) $\lceil\alpha\{|\ (\sqcup i\in I\cdot S_i)\ |\}\beta\rceil=(\sqcap\sigma:\Sigma\cdot(\sqcup i\in I\cdot\lceil\alpha\mid\sigma\{|\ S_i\ |\}\beta\rceil))$, where it is supposed that $(\sqcup i\in I\cdot S_i)$ is well-defined, and for each $\sigma:\Sigma$, $\alpha\mid\sigma:\mathbf{P}\Sigma$ denotes the restriction of α at σ and it is defined by

$$(\alpha\mid\sigma).\sigma'=\begin{cases}\alpha.\sigma\text{ if }\sigma'=\sigma,\\ 0\text{ if }\sigma'\in\Sigma-\{\sigma\}.\end{cases}$$

(5) $\lceil\alpha\{|\ (\sqcap i\in I\cdot S_i)\ |\}\beta\rceil=(\sqcap i\in I\cdot\lceil\alpha\{|\ S_i\ |\}\beta\rceil)$.

Proof. (1) It follows that

$$\begin{aligned}\lceil\alpha\{|\ \{R\}\ |\}\beta\rceil &= \lceil\alpha\equiv>\{R\}.\beta\rceil\\ &= \left(\sqcap\sigma:\Sigma\cdot\min\left[1,\frac{(\{R\}.\beta).\sigma}{\alpha.\sigma}\right]\right)\\ &= \left(\sqcap\sigma:\Sigma\cdot\min\left[1,\frac{(\sqcup\gamma:\Gamma.R.\sigma.\gamma\times\beta.\gamma)}{\alpha.\sigma}\right]\right)\end{aligned}$$

$$
\begin{aligned}
&= \left(\sqcap\sigma : \Sigma \cdot \min\left[1, \left(\sqcup\gamma : \Gamma \cdot \frac{R.\sigma.\gamma \times \beta.\gamma}{\alpha.\sigma}\right)\right]\right) \\
&= \left(\sqcap\sigma : \Sigma \cdot \left(\sqcup\gamma : \Gamma \cdot \min\left[1, \frac{R.\sigma.\gamma \times \beta.\gamma}{\alpha.\sigma}\right]\right)\right) \\
&= \left(\sqcup f{:}\Sigma \to \Gamma \cdot \left(\sqcap\sigma{:}\Sigma \cdot \min\left[1, \frac{R.\sigma.(f.\sigma) \times \beta.(f.\sigma)}{\alpha.\sigma}\right]\right)\right) \\
&= (\sqcup f : \Sigma \to \Gamma \cdot \lceil \alpha \equiv> (R; f) \times (\beta; f) \rceil.
\end{aligned}
$$

Note that the complete distributivity

$$
(\sqcap i : I \cdot (\sqcup j : J_j \cdot a_{ij})) = \left(\sqcup f : \prod_{i\in I} J_i \cdot \left(\sqcap i : I \cdot a_{if(i)}\right)\right)
$$

of $\sqcap$ over $\sqcup$ is applied in the equality before the last one.
(2) We have

$$
\begin{aligned}
\lceil \alpha\{|\ [R]\ |\}\beta \rceil &= \lceil \alpha \equiv> [R].\beta \rceil \\
&= \left(\sqcap\sigma : \Sigma \cdot \min\left[1, \frac{([R].\beta).\sigma}{\alpha.\sigma}\right]\right) \\
&= \left(\sqcap\sigma : \Sigma \cdot \min\left[1, \frac{\left(\sqcap\gamma : \Gamma \cdot \min\left(1, \frac{\beta.\gamma}{R.\sigma.\gamma}\right)\right)}{\alpha.\sigma}\right]\right) \\
&= \left(\sqcap\sigma{:}\Sigma \cdot \min\left[1, \left(\sqcap\gamma{:}\Gamma \cdot \min\left(\frac{1}{\alpha.\sigma}, \frac{\beta.\gamma}{\alpha.\sigma \times R.\sigma.\gamma}\right)\right)\right]\right) \\
&= \left(\sqcap\sigma : \Sigma \cdot \sqcap\gamma : \Gamma \cdot \min\left[1, \frac{1}{\alpha.\sigma}, \frac{\beta.\gamma}{\alpha.\sigma \times R.\sigma.\gamma}\right]\right),
\end{aligned}
$$

and

$$
\begin{aligned}
\lceil ran.(|\ \alpha\ |; R) \equiv> \beta \rceil &= \left(\sqcap\gamma : \Gamma \cdot \min\left[1, \frac{\beta.\gamma}{ran.(|\ \alpha\ |; R).\gamma}\right]\right) \\
&= \left(\sqcap\gamma : \Gamma \cdot \min\left[1, \frac{\beta.\gamma}{(\sqcup\sigma : \Sigma \cdot \alpha.\sigma \times R.\sigma.\gamma)}\right]\right) \\
&= \left(\sqcap\gamma : \Gamma \cdot \min\left[1, \left(\sqcap\sigma : \Sigma \cdot \frac{\beta.\gamma}{\alpha.\sigma \times R.\sigma.\gamma}\right)\right]\right) \\
&= \left(\sqcap\gamma : \Gamma \cdot \sqcap\sigma : \Sigma \cdot \min\left[1, \frac{\beta.\gamma}{\alpha.\sigma \times R.\sigma.\gamma}\right]\right).
\end{aligned}
$$

Then the condition that $\alpha.\sigma \leq 1$ for all $\sigma : \Sigma$ implies that

$$
\lceil \alpha\{|\ [R]\ |\}\beta \rceil = \lceil ran.(|\ \alpha\ |; R) \equiv> \beta \rceil.
$$

(3) First, it holds that

$$\begin{aligned}\lceil \alpha\{|\ S_1; S_2\ |\}\theta\rceil &= \lceil \alpha \equiv\!> (S_1; S_2).\theta\rceil \\ &= \lceil \alpha \equiv\!> S_1.(S_2.\theta)\rceil \\ &= \lceil \alpha \equiv\!> S_1.(S_2.\theta)\rceil \times \lceil S_2.\theta \equiv\!> S_2.\theta)\rceil \\ &= \lceil \alpha\{|\ S_1\ |\}S_2.\theta\rceil \times \lceil S_2.\theta\{|\ S_2\ |\}\theta\rceil \\ &\leq \text{ the right} - \text{hand side.}\end{aligned}$$

Conversely, if S_1 is strongly monotone, then for any $\beta : \mathbf{P}\Gamma$ we have

$$\begin{aligned}\lceil \alpha\{|\ S_1\ |\}\beta\rceil \times \lceil \beta\{|\ S_2\ |\}\theta\rceil &= \lceil \alpha \equiv\!> S_1.\beta\rceil \times \lceil \beta \equiv\!> S_2.\theta\rceil \\ &\leq \lceil \alpha \equiv\!> S_1.\beta\rceil \times \lceil S_1.\beta \equiv\!> S_1.(S_2.\theta)\rceil \\ &\leq \lceil \alpha \equiv\!> S_1.(S_2.\theta)\rceil \\ &= \lceil \alpha\{|\ S_1; S_2\ |\}\theta\rceil,\end{aligned}$$

and this completes the proof of (3).
(4) and (5) may be simply carried out by the related definitions.#

7 Probabilistic predicate transformer semantics and choice semantics of contracts

The aim of this section is to present two probabilistic semantical models of R. -J. Back and J. von Wright's contract language [4]. The contract language is an extension of E. W. Dijkstra's guarded command language, and it contains both angelic and demonic nondeterminism. The syntax of contracts is given by

$$S ::= \{R\} \mid [R] \mid S_1; S_2 \mid (\sqcap i \in I \cdot S_i) \mid (\sqcup i \in I \cdot S_i),$$

where R is a probabilistic relation, I is an index set, and S, S_1, S_i and S_i $(i \in I)$ range over contract statements. Note that an infinite join of probabilistic predicate transformers need not to be a probabilistic predicate transformer because it may be unbounded. The boundedness of a probabilistic predicate transformer is not decidable at the level of syntax. So, in what follows we always suppose that the index set I in an angelic choice is finite. It should be pointed out that recursion is not included in the contract language considered in this paper.

The first semantical model that we are going to give to contracts is probabilistic predicate transformer semantics. For each contract statement S, the semantics gives a probabilistic predicate transformer $wp.S$. $wp.S$ is defined by induction on the structure of S :
(1) If $R : \Sigma \leftrightarrow \Gamma$, then

$$wp.\{R\} := \{R\} \text{ and } wp.[R] := [R].$$

Note that $\{R\}$ and $[R]$ in the left-hand side are contract statements, but $\{R\}$ and $[R]$ in the right-hand side are probabilistic updates given in Definition 6, and they are probabilistic predicate transformers in $\Sigma \mapsto \Gamma$.
(2) $wp.(S_1; S_2) := wp.S_1; wp.S_2$.
(3) $wp.(\sqcap i \in I \cdot S_i) := (\sqcap i \in I \cdot wp.S_i)$.
(4) $wp.(\sqcup i \in I \cdot S_i) := (\sqcup i \in I \cdot wp.S_i)$.

The other semantical model that we are going to introduce in this section is probabilistic choice semantics. The probabilistic choice semantics $ch.S$ of a contract statement S is defined by induction on the structure of S.
(1) Let $R : \Sigma \leftrightarrow \Gamma$. Then for all $\sigma : \Sigma$ and $\alpha : \mathbf{P}\Gamma$,

$$ch.\{R\}.\sigma.\alpha := height(R.\sigma \times \alpha),$$

where for each $\beta : \mathbf{P}\Gamma$,

$$height(\beta) := (\sqcup \gamma : \Gamma.\beta.\gamma).$$

(2) Let $R : \Sigma \leftrightarrow \Gamma$. Then for all $\sigma : \Sigma$ and $\alpha : \mathbf{P}\Gamma$,

$$ch.[R].\sigma.\alpha := \lceil R.\sigma \equiv > \alpha \rceil.$$

(3) Let $S_1 : \Sigma \mapsto \Gamma$ and $S_2 : \Gamma \mapsto \Delta$. Then for any $\sigma : \Sigma$,

$$ch.(S_1; S_2).\sigma := \left(\sqcup \alpha : \mathbf{P}\Gamma \cdot ch.S_1.\sigma.\alpha \times \left(\sqcap \gamma : \Gamma \cdot \min \left[1, \frac{ch.S_2.\gamma}{\alpha.\gamma} \right] \right) \right).$$

(4) Let $S_i \, (i \in I) : \Sigma \mapsto \Gamma$. Then for any $\sigma : \Sigma$,

$$ch.(\sqcap i \in I \cdot S_i).\sigma := (\sqcap i \in I \cdot ch.S_i.\sigma).$$

(5) Let $S_i \, (i \in I) : \Sigma \mapsto \Gamma$. Then for any $\sigma : \Sigma$,

$$ch.(\sqcup i \in I \cdot S_i).\sigma := (\sqcup i \in I \cdot ch.S_i.\sigma).$$

The probabilistic predicate transformer semantics and choice semantics for contracts are closely related to each other. To show their connection, we first introduce a variant of probabilistic predicate transformers. Let Σ and Γ be two state spaces and $t : \Sigma \mapsto \Gamma$. Then the currying of t is a mapping $\bar{t} : \Sigma \mapsto \mathbf{P}\Gamma \to \mathbf{R}_{\geq}$ and it is defined by

$$\bar{t}.\sigma.\alpha := t.\alpha.\sigma$$

for all $\alpha : \Sigma$ and $\alpha : \mathbf{P}\Gamma$. It is easy to see that "$-$" is an one-one function from $\Sigma \mapsto \Gamma$ onto the mappings $\psi : \Sigma \mapsto \mathbf{P}\Gamma \to \mathbf{R}_{\geq}$ such that for each $\alpha : \mathbf{P}\Gamma$, there is $M \in \mathbf{R}_{\geq}$ with $\psi.\sigma.\alpha \leq M$ for all $\sigma : \Sigma$.

One of the most important properties that we impose on probabilistic predicate is strong monotonicity. It is interesting that as showed in Proposition 32 below, strong monotonicity of a probabilistic predicate transformer is equivalent to a certain closedness of its currying, defined by the following:

Definition 14. *Let Σ be a state space and $K : \mathbf{P}\Sigma \to \mathbf{R}_{\geq}$ a mapping. Then K is said to be upward closed if for all $\alpha, \beta : \mathbf{P}\Sigma$,*

$$K.\alpha \times \lceil \alpha \equiv\!> \beta \rceil \leq K.\beta.$$

Proposition 32. *Let Σ and Γ be state spaces and $t : \Sigma \mapsto \Gamma$. Then t is strongly monotonic if and only if $\overline{t}.\sigma$ is upward closed for all $\sigma : \Sigma$.*

Proof. ($\Rightarrow$) Since t is strongly monotone, we obtain for any $\alpha, \beta : \mathbf{P}\Gamma$,

$$\begin{aligned}
\overline{t}.\sigma.\alpha \times \lceil \alpha \equiv\!> \beta \rceil &= t.\alpha.\sigma \times \lceil \alpha \equiv\!> \beta \rceil \\
&\leq t.\alpha.\sigma \times \lceil t.\alpha \equiv\!> t.\beta \rceil \\
&= t.\alpha.\sigma \times \left(\sqcap \sigma' : \Sigma \cdot \min\left(1, \frac{t.\beta.\sigma'}{t.\alpha.\sigma'}\right)\right) \\
&\leq t.\alpha.\sigma \times \frac{t.\beta.\sigma}{t.\alpha.\sigma} \\
&= t.\beta.\sigma \\
&= \overline{t}.\sigma.\beta.
\end{aligned}$$

This means that $\overline{t}.\sigma$ is upward closed.

($\Leftarrow$) From the upward closedness of $\overline{t}.\sigma$ it follows that

$$\begin{aligned}
\lceil t.\alpha \equiv\!> t.\beta \rceil &= \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{t.\beta.\sigma}{t.\alpha.\sigma}\right)\right) \\
&= \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{\overline{t}.\sigma.\beta}{\overline{t}.\sigma.\alpha}\right)\right) \\
&\geq \left(\sqcap \sigma : \Sigma \cdot \min\left(1, \frac{\overline{t}.\sigma.\alpha \times \lceil \alpha \equiv\!> \beta \rceil}{\overline{t}.\sigma.\alpha}\right)\right) \\
&= \lceil \alpha \equiv\!> \beta \rceil.
\end{aligned}$$

So, t is strongly monotone.#

Probabilistic refinement of probabilistic predicate transformers may be expressed in terms of probabilistic implication between their curryings.

Proposition 33. *Let Σ and Γ be state spaces and $t, t' : \Sigma \mapsto \Gamma$. Then*

$$\lceil t \sqsubseteq t' \rceil = (\sqcap \sigma : \Sigma \cdot \lceil \overline{t}.\sigma \equiv\!> \overline{t'}.\sigma \rceil).$$

Proof. Straightforward from the related definitions.#

After introducing the currying construct, we are able to establish a one-to-one correspondence between probabilistic predicate transformer semantics and choice semantics.

Proposition 34. *For any contract statement* S, $ch.S = \overline{wp.S}$.

Proof. We proceed by induction on the structure of S. For simplicity, we only deal with the case of sequential composition. Our purpose here is to show that for any $\sigma : \Sigma$ and $\beta : \mathbf{P}\Delta$,

$$ch.(S_1; S_2).\sigma.\beta = \overline{wp.(S_1; S_2)}.\sigma.\beta.$$

From item (3) in the definition of $ch.S$ it follows that

$$ch.(S_1; S_2).\sigma.\beta \geq ch.S_1\sigma.(wp.S_2.\beta) \times \left(\sqcap\gamma : \Gamma \cdot \min\left[1, \frac{ch.S_2.\gamma.\beta}{wp.S_2.\beta.\gamma}\right]\right).$$

With the induction hypothesis on S_2, we have

$$ch.S_2.\gamma.\beta = \overline{wp.S_2}.\gamma.\beta = wp.S_2.\beta.\gamma.$$

This yields

$$ch.(S_1; S_2).\sigma.\beta \geq ch.S_1\sigma.(wp.S_2.\beta).$$

Furthermore, we use the induction hypothesis on S_1 and obtain

$$\begin{aligned} ch.(S_1; S_2).\sigma.\beta &\geq \overline{wp.S_1}.\sigma.(wp.S_2.\beta) \\ &= wp.S_1.(wp.S_2.\beta).\sigma \\ &= wp.(S_1; S_2).\beta.\sigma \\ &= \overline{wp.(S_1; S_2)}.\sigma.\beta. \end{aligned}$$

Conversely, for any $\alpha : \mathbf{P}\Gamma$, we write

$$N(\alpha) = ch.S_1.\sigma.\alpha \times \left(\sqcap\gamma : \Gamma \cdot \min\left[1, \frac{ch.S_2.\gamma.\beta}{\alpha.\gamma}\right]\right).$$

Then the induction hypothesis asserts that

$$\begin{aligned} N(\alpha) &= wp.S_1.\alpha.\sigma \times \left(\sqcap\gamma : \Gamma. \min\left[1, \frac{wp.S_2.\beta.\gamma}{\alpha.\gamma}\right]\right) \\ &= wp.S_1.\alpha.\sigma \times \lceil \alpha \equiv> wp.S_2.\beta \rceil. \end{aligned}$$

Since $wp.S_1$ is strongly monotone (see Lemma 11), we have

$$\begin{aligned}
N(\alpha) &\leq wp.S_1.\alpha.\sigma \times \lceil wp.S_1.\alpha \equiv\!> wp.S_1.(wp.S_2.\beta)\rceil \\
&= wp.S_1.\alpha.\sigma \times \lceil wp.S_1.\alpha \equiv\!> wp.(S_1;S_2).\beta\rceil \\
&= wp.S_1.\alpha.\sigma \times \left(\sqcap\sigma' : \Sigma \cdot \min\left[1, \frac{wp(S_1;S_2).\beta.\sigma'}{wp.S_1.\alpha.\sigma'}\right]\right) \\
&\leq wp.S_1.\alpha.\sigma \times \frac{wp(S_1;S_2).\beta.\sigma}{wp.S_1.\alpha.\sigma} \\
&= wp(S_1;S_2).\beta.\sigma \\
&= \overline{wp(S_1;S_2)}.\sigma.\beta.\#
\end{aligned}$$

Note that the second part of the above proof appeals to the strong monotonicity of probabilistic predicate transformers, and the weak monotonicity is not sufficient.

To conclude this section, we briefly compare probabilistic choice semantics with J. He, K. Seidel and A. McIver's relational semantical model for probabilistic programs [12]. Note that $\mathbf{C}\Gamma \subseteq \mathbf{P}\Gamma$. If we identify each subset U of $\mathbf{C}\Gamma$ with its characteristic function

$$\chi_U.\alpha = \begin{cases} 1 \text{ if } \alpha \in U, \\ 0 \text{ if } \alpha \in \mathbf{P}\Gamma - U, \end{cases}$$

then $\mathbf{P}(\Sigma, \Gamma) \subseteq \Sigma \to \mathbf{P}\Gamma \to R_{\geq}$. Moreover, it is easy to see that the relational semantics and choice semantics will give the same models for their common program constructs. In a sense, the choice semantics may be seen as an extension of the relational semantical model.

8 Probabilistic game semantics of contracts

R. -J. Back and J. von Wright [4] proposed a game semantics of their contract language where a contract statement is interpreted as a game played between two opponents, angel and demon. The game semantics is an operational semantical model and it describes how a contract statement encodes the rules of a game. They established a winning strategy theorem which says that an initial state satisfies the weakest precondition of a postcondition if and only if the angel has a winning strategy from the initial state to reach a final state fulfilling the postcondition. Thus, the predicate transformer semantics can be derived from the game semantics, and the former is an abstraction of the latter. In this section, we want to give a probabilistic generalization of R. -J. Back and J. von Wright's game semantics. To this end, we first introduce a probabilistic transitional semantics of contract statements. We call a pair of the form (S, σ) a configuration, where S is a contract statement

or Λ standing for empty string of symbols, σ is a state in the state space under consideration, the symbol $\top$ for success, or $\bot$ for failure. The transitional semantics consists of weighted transitions between configurations. A weighted transition is of the form $(S, \sigma) \xrightarrow{w} (S', \sigma')$ in which $w \in \mathbf{R}_{\geq}$ is called weight of the transition. The intuitive meaning of weight will be given together with the interpretation of transition rules below. Such a transition will be abbreviated to $(S, \sigma) \longrightarrow (S', \sigma')$ whenever $w = 1$. The transitional semantics is presented in G. D Plotkin's style of SOS (structured operational semantics) [35], and it is given by the following transition rules:

Angelic update

$$\frac{}{(\{R\}, \sigma) \xrightarrow{R.\sigma.\gamma} (\Lambda, \gamma)}$$

$$\frac{}{(\{R\}, \bot) \longrightarrow (\Lambda, \bot)}$$

$$\frac{}{(\{R\}, \top) \longrightarrow (\Lambda, \top)}$$

Demonic update

$$\frac{}{([R], \sigma) \xrightarrow{R.\sigma.\gamma} (\Lambda, \gamma)}$$

$$\frac{}{([R], \bot) \longrightarrow (\Lambda, \bot)}$$

$$\frac{}{([R], \top) \longrightarrow (\Lambda, \top)}$$

Sequential composition

$$\frac{(S_1, \sigma) \xrightarrow{\lambda} (S_1', \gamma), \qquad S_1' \neq \Lambda}{(S_1; S_2, \sigma) \xrightarrow{\lambda} (S_1'; S_2, \gamma)}$$

$$\frac{(S_1, \sigma) \xrightarrow{\lambda} (\Lambda, \gamma)}{(S_1; S_2, \sigma) \xrightarrow{\lambda} (S_2, \gamma)}$$

Angelic choice

$$\frac{}{(S_1 \sqcup S_2, \sigma) \longrightarrow (S_1, \sigma)}$$

$$\frac{}{(S_1 \sqcup S_2, \sigma) \longrightarrow (S_2, \sigma)}$$

Demonic choice

$$\frac{k \in I}{((\sqcap i \in I \cdot S_i), \sigma) \longrightarrow (S_k, \sigma)}$$

$$\frac{I \neq \phi}{((\sqcap i \in I \cdot S_i), \sigma) \longrightarrow (\Lambda, \top)}$$

All of the above rules except the first rule for angelic and demonic updates are similar to the corresponding ones for non-probabilistic contract statements, and they do not deserve any further explanation. For a better understanding of the first rule for probabilistic angelic update, we compare it with the corresponding rules for the non-probabilistic update. In the non-probabilistic case, there are two rules for angelic update starting from a proper state (not success symbol $\top$ and failure $\bot$), and they read

$$\frac{R.\sigma.\gamma}{(\{R\}, \sigma) \to (\Lambda, \gamma)}$$

$$\frac{R.\sigma = \phi}{(\{R\}, \sigma) \to (\Lambda, \bot)}$$

It is obvious that the rule for probabilistic update is an imitation of the first of the above non-probabilistic rules. However, the latter has a premise, and the former does not. This seems a big difference between them at the first glance. Indeed, in the probabilistic rule, the premise is implicitly embedded into the conclusion sequent and it is indicated by a positive weight. The second non-probabilistic rule deals with the case that there is no state satisfying relation R with σ. The probabilistic cousin of this case is that $R.\sigma.\gamma = 0$ for all γ. It is merged with the case that $R.\sigma.\gamma > 0$ for some γ into a single rule, and signalled by a zero weight. The weights of the involved transitions will be computed in the evaluation of the winning index of a strategy. A similar explanation is due to the first rule of probabilistic demonic update.

Similar to the non-probabilistic case, the behavior of a probabilistic contract is described by its plays. A play of probabilistic contract statement S in initial state σ is a sequence of transitions

$$C_0 \stackrel{\lambda_1}{\to} C_1 \stackrel{\lambda_2}{\to} C_2 \stackrel{\lambda_3}{\to} ... \stackrel{\lambda_n}{\to} C_n$$

where

(i) $C_0 = (S, \sigma)$, and

(ii) if the sequence is finite, then it ends with an empty configuration.

In a way like Lemma 14.1 in [4], we may show that all plays of a probabilistic contracts (without recursive constructs) are finite. This enables us to define the notion of winning for probabilistic games by induction on the length of plays. The notion of winning for probabilistic games is much more complicated that that for non-probabilistic games. We define winning index to indicate the possibility that the angel wins the game. Let α be a probabilistic predicate on the state space Σ. The winning index $win(\rho, \alpha)$ of a finite play

$$\rho = C_0 \stackrel{\lambda_1}{\to} C_1 \stackrel{\lambda_2}{\to} C_2 \stackrel{\lambda_3}{\to} ... \stackrel{\lambda_n}{\to} C_n$$

with respect to a goal α is defined by induction on the length n of ρ :
(1) If $n = 0$, and $C_0 = (S, \sigma)$, then

$$win(\rho, \alpha) = \begin{cases} \alpha.\sigma \text{ if } \sigma : \Sigma, \\ 1 \text{ if } \sigma = \top, \\ 0 \text{ if } \sigma = \bot . \end{cases}$$

(2) In general, we write the tail of ρ as

$$\rho' = C_1 \stackrel{\lambda_2}{\to} C_2 \stackrel{\lambda_3}{\to} ... \stackrel{\lambda_n}{\to} C_n,$$

and suppose that $win(\rho', \alpha)$ is already defined. Then

$$win(\rho,\alpha) = \begin{cases} \lambda_1 \times win(\rho', \alpha) \text{ if } C_0 \text{ is an angelic update configuration,} \\ \min\left(1, \frac{win(\rho', \alpha)}{\lambda_1}\right) \text{ if } C_0 \text{ is a demonic update configuration,} \\ win(\rho', \alpha) \text{ otherwise.} \end{cases}$$

The notions of strategy and admission of probabilistic games are very similar to the corresponding notion for non-probabilistic games. A strategy is a function f from configurations to themselves such that for all angelic configurations C, $C \xrightarrow{\lambda} f.C$ for some $\lambda \in \mathbf{R}_{\geq}$.

The strategy f admits play $C_0 \xrightarrow{\lambda_1} C_1 \xrightarrow{\lambda_2} C_2 \xrightarrow{\lambda_3} ... \xrightarrow{\lambda_n} C_n$ of S in initial state σ if $C_{i+1} = f.C_i$ whenever C_i is an angelic configuration for all $i \leq n$.

With the help of the concepts introduced above, we are able to define a graded notion of winning for probabilistic game strategies. The winning index of strategy f for S in initial state σ with respect to goal α is defined as

$$win(f \mid S, \sigma, \alpha) = (\sqcap \rho \mid \rho \text{ is a play of } S \text{ in } \sigma \text{ admitted by } f \cdot win(\rho, \alpha)).$$

We now are ready to present the main result of this section, the winning strategy theorem of probabilistic contracts. This theorem considerably generalizes Theorem 14.2 in [4].

Theorem 35. *Let S be a probabilistic contract statement (without recursions and iterations) , σ a state in Σ, and $\alpha : \mathbf{P}\Gamma$, where Σ and Γ are suitable state spaces. Then*

$$wp.S.\alpha.\sigma = (\sqcup f \mid f \text{ is a strategy} \cdot win(f \mid S, \sigma, \alpha)).$$

Proof. For simplicity, we write $g(S, \sigma, \alpha)$ for the right-hand side of the above equality. We proceed by induction on the length of statement S.

Case 1. $S = \{R\}$. For any $\gamma : \Gamma$, we write f_γ for a strategy with $f_\gamma.(\{R\}, \sigma) = (\Lambda, \gamma)$. The unique play of S in σ admitted by f_γ is

$$\rho_\gamma = (\{R\}, \sigma) \xrightarrow{R.\sigma.\gamma} (\Lambda, \gamma)$$

and it is easy to see that

$$win(f_\gamma \mid S, \sigma, \alpha) = win(\rho_\gamma, \alpha) = R.\sigma.\gamma \times \alpha.\gamma.$$

Then

$$\begin{aligned} g(S, \alpha, \sigma) &= (\sqcup \gamma : \Gamma \cdot win(f_\gamma \mid S, \sigma, \alpha)) \\ &= (\sqcup \gamma : \Gamma \cdot R.\sigma.\gamma \times \alpha.\gamma) \\ &= \{R\}.\alpha.\sigma \\ &= wp.S.\alpha.\sigma. \end{aligned}$$

Case 2. $S = [R]$. For all $\gamma : \Gamma$, the play

$$\rho_\gamma = ([R], \sigma) \xrightarrow{R.\sigma.\gamma} (\Lambda, \gamma)$$

of S in σ is admitted by every strategy f. Moreover, from the definition of winning index we have

$$\begin{aligned} win(f \mid S, \sigma, \alpha) &= (\sqcap \gamma : \Gamma \cdot win(\rho_\gamma, \alpha)) \\ &= \left(\sqcap \gamma : \Gamma \cdot \min\left(1, \frac{\alpha.\gamma}{R.\sigma.\gamma}\right)\right) \\ &= [R].\alpha.\sigma. \end{aligned}$$

Note that the right-hand side of the above equality does not depend on the choice of strategy f. Thus, it follows that

$$g(S, \alpha, \sigma) = [R].\alpha.\sigma = wp.S.\alpha.\sigma.$$

Case 3. $S = S_1 \sqcup S_2$. For any strategy f, and for any play ρ of S_1 in σ admitted by f, we set f_1 to be a modification of f so that f_1 is the same as f except at $(S_1 \sqcup S_2, \sigma)$ and $f_1.(S_1 \sqcup S_2, \sigma) = (S_1, \sigma)$, and $\rho_1 = (S_1 \sqcup S_2, \sigma) \longrightarrow \rho$. Then we know that ρ_1 is a play of $S_1 \sqcup S_2$ in σ and admitted by f_1, and $win(\rho, \alpha) = win(\rho_1, \alpha)$. Furthermore, it follows that

$$win(f_1 \mid S_1 \sqcup S_2, \sigma, \alpha) = win(f \mid S_1, \sigma, \alpha).$$

Likewise, we can construct a strategy f_2 and a play ρ_2 of $S_1 \sqcup S_2$ in σ admitted by f_2 from each strategy f and each play ρ of S_2 in σ admitted by f. With the induction hypothesis, we obtain

$$\begin{aligned} wp.S.\alpha.\sigma &= \max(wp.S_1.\alpha.\sigma, wp.S_2.\alpha.\sigma) \\ &= \max((\sqcup f \mid f \text{ is a strategy} \cdot win(f \mid S_1, \sigma, \alpha)), \\ &\quad (\sqcup f \mid f \text{ is a strategy} \cdot win(f \mid S_2, \sigma, \alpha))) \\ &= \max((\sqcup f \mid f \text{ is a strategy} \cdot win(f_1 \mid S_1 \sqcup S_2, \sigma, \alpha)), \\ &\quad (\sqcup f \mid f \text{ is a strategy} \cdot win(f_2 \mid S_1 \sqcup S_2, \sigma, \alpha))) \\ &= g(S, \alpha, \sigma). \end{aligned}$$

Case 4. $S = (\sqcap i \in I \cdot S_i)$. We write K for the set of all strategies. Then the induction hypothesis leads to

$$\begin{aligned} wp.S.\alpha.\sigma &= (\sqcap i \in I \cdot wp.S_i.\alpha.\sigma) \\ &= (\sqcap i \in I \cdot (\sqcup f_i \mid f_i \text{ is a strategy} \cdot win(f_i \mid S_i, \sigma, \alpha))) \\ &= (\sqcup h \in K^I \cdot (\sqcap i \in I \cdot win(h.i \mid S_i, \sigma, \alpha))). \end{aligned}$$

First, we observe that for any play ρ_i of S_i in σ admitted by f, $\rho = (S, \sigma) \longrightarrow \rho_i$ is a play of S in σ admitted by f and $win(\rho, \alpha) = win(\rho_i, \alpha)$.

Thus,

$$\begin{aligned} win(f \mid S, \sigma, \alpha) &= (\sqcap \rho \mid \rho \text{ is a play of } S \text{ in } \sigma \text{admitted by } f \cdot win(\rho, \alpha)) \\ &= (\sqcap i \in I \cdot (\sqcap \rho_i \mid \rho_i \text{ is a play of } S_i \text{ in } \sigma \\ &\quad \text{admitted by } f \cdot win(\rho_i, \alpha))) \\ &= (\sqcap i \in I \cdot win(f \mid S_i, \sigma, \alpha)). \end{aligned}$$

Furthermore, for any $f \in K$, we use $\overline{f}$ to denote the constant function in K^I with $\overline{f}.i = f$ for all $i \in I$. Then we have

$$\begin{aligned} wp.S.\alpha.\sigma &\geq (\sqcup f \in K \cdot (\sqcap i \in I \cdot win(\overline{f}.i \mid S_i, \sigma, \alpha))) \\ &= (\sqcup f \in K \cdot (\sqcap i \in I \cdot win(f \mid S_i, \sigma, \alpha))) \\ &= (\sqcup f \in K \cdot win(f \mid S, \sigma, \alpha)) \\ &= g(S, \alpha, \sigma). \end{aligned}$$

Conversely, for any $h \in K^I$, we define a strategy h^* such that $h^*.C = h.i.C$ whenever C appears in a play of S_i in σ. Indeed, h^* is a merge of $\{h.i \mid i \in I\}$ according to the part (iii) of the proof of Theorem 14.2 in [4]. It is easy to note that ρ is a play of S in σ admitted by h^* if and only if for some $i \in I$, $\rho = (S, \sigma) \longrightarrow \rho_i$ and ρ_i is a play of S_i in σ admitted by $h.i$; and in this case, $win(\rho, \alpha) = win(\rho_i, \alpha)$. This yields

$$win(h^* \mid S, \sigma, \alpha) = (\sqcap i \in I \cdot win(h.i \mid S_i, \sigma, \alpha)).$$

Therefore,

$$\begin{aligned} wp.S.\alpha.\sigma &= (\sqcup h \in K^I \cdot win(h^* \mid S, \sigma, \alpha)) \\ &\leq (\sqcup f \in K \cdot win(f \mid S, \sigma, \alpha)) \\ &= g(S, \alpha, \sigma). \end{aligned}$$

Case 5. $S = S_1; S_2$. From the induction hypothesis for S_2 we know that for all $\delta : \Delta$,

$$wp.S_2.\alpha.\delta = (\sqcup f \mid f \text{ is a strategy} \cdot win(f \mid S_2, \delta, \alpha)),$$

where Δ is a suitable state space. We define a function $win(f \mid S_2, ., \alpha)$ from Δ to $\mathbf{R}_{\geq}$ with $win(f \mid S_2, ., \alpha).\delta = win(f \mid S_2, \delta, \alpha)$ for all $\delta : \Delta$. Then for any play ρ of S_1 in σ we can use induction on the length of ρ to show that

$$win(\rho, wp.S_2.\alpha) = (\sqcup f \mid f \text{ is a strategy} \cdot win(\rho, win(f \mid S_2, ., \alpha))).$$

Here the infinite distributivity of multiplication over $\sqcup$ is applied in the induction stage. Now for each strategy g,

$$\begin{aligned} &win(g \mid S_1, \sigma, wp.S_2.\alpha) = (\sqcap\rho \mid \rho \text{ is a play of } S_1 \text{ in } \sigma \\ &\quad \text{admitted by } g \cdot win(\rho, wp.S_2.\alpha)) \\ &= (\sqcap\rho \mid \rho \text{ is a play of } S_1 \text{ in } \sigma \text{admitted by } g \cdot (\sqcup f \mid f \\ &\quad \text{is a strategy} \cdot win(\rho, win(f \mid S_2, ., \alpha)))) \\ &= (\sqcup h \in K^{p(S_1,\sigma,g)} \cdot (\sqcap\rho \in p(S_1, \sigma, g) \cdot win(\rho, win(h.\rho \mid S_2, ., \alpha)))), \end{aligned}$$

where K is the set of strategy, and $p(S_1, \sigma, g)$ the set of plays of S_1 in σ admitted by g. Furthermore, using the induction hypothesis for S_1 we obtain

$$\begin{aligned} wp.(S_1; S_2).\alpha.\sigma &= (wp.S_1; wp.S_2).\alpha.\sigma \\ &= wp.S_1.(wp.S_2.\alpha).\sigma \\ &= (\sqcup g \in K \cdot win(g \mid S_1, \sigma, wp.S_2.\alpha)) \\ &= (\sqcup g \in K, h \in K^{p(S_1,\sigma,g)} \cdot (\sqcap\rho \in p(S_1, \sigma, g) \\ &\quad \cdot \ win(\rho, win(h.\rho \mid S_2, ., \alpha)))). \end{aligned}$$

Note that

$$win(h.\rho \mid S_2, \delta, \alpha) = (\sqcap\tau \in p(S_2, \delta, h.\rho) \cdot win(\tau, \alpha))$$

for all δ. For any play $\rho = (S_1, \sigma) \to ... \to (\Lambda, \delta)$ of S_1 in σ and any play $\tau = (S_2, \delta) \to ... \to C_0$, we write $\rho; S_2 \to \tau$ for the play $(S_1; S_2, \sigma) \to ... \to (S_2, \delta) \to ... \to C_0$. Then with the infinite distributivity of multiplication over $\sqcap$ and induction on the length of ρ we can prove that

$$win(\rho, win(h.\rho \mid S_2, ., \alpha)) = (\sqcap\tau \in p(S_2, \delta, h.\rho) \cdot win(\rho; S_2 \to \tau, \alpha)).$$

Consequently, it holds that

$$\begin{aligned} &wp.(S_1; S_2).\alpha.\sigma = (\sqcup g \in K, h \in K^{p(S_1,\sigma,g)} \cdot (\sqcap\rho \in p(S_1, \sigma, g), \\ &\tau \in p(S_2, \delta, h.\rho) \ \cdot \ win(\rho; S_2 \to \tau, \alpha))). \end{aligned}$$

For any $g \in K$ and $h \in K^{p(S_1,\sigma,g)}$, we define a strategy $g \oplus h$ in the following way:

$(g \oplus h).(S; S_2, \delta) := g.(S, \delta)$ if (S, δ) appears in a play of S_1 in σ;

$(g \oplus h).(S, \gamma) := h.\rho.(S, \gamma)$ if (S, γ) appears in a play of S_2 in the target state of ρ.

We note that $\mu \in p(S_1; S_2, \sigma, g \oplus h)$ if and only if $\mu = \rho; S_2 \to \tau$ for some $\rho \in p(S_1, \sigma, g)$ and $\tau \in p(S_2, \delta, h.\rho)$, where δ is the target state of ρ.

This finally yields

$$\begin{aligned} wp.(S_1; S_2).\alpha.\sigma &= (\sqcup f \in K \cdot (\sqcap \mu \in p(S_1; S_2, \sigma, f) \cdot win(\mu, \alpha)) \\ &= (\sqcup f \in K \cdot win(f \mid S_1; S_2, \sigma, \alpha)) \\ &= g(S_1; S_2, \sigma, \alpha).\# \end{aligned}$$

We may observe that the proof of the above theorem heavily depends on three distributivities of reals: for all real numbers$a$, a_i $(i \in I)$, and a_{ij} $(i \in I, j \in J_i)$,
(1) complete distributivity between $\sqcap$ and $\sqcup$:

$$(\sqcap i \in I \cdot (\sqcup j \in J_j \cdot a_{ij})) = \left(\sqcup f \in \prod_{i \in I} J_i \cdot \left(\sqcap i \in I \cdot a_{if(i)} \right) \right),$$

$$(\sqcup i \in I \cdot (\sqcap j \in J_j \cdot a_{ij})) = \left(\sqcap f \in \prod_{i \in I} J_i \cdot \left(\sqcup i \in I \cdot a_{if(i)} \right) \right);$$

(2) infinite distributivity of multiplication over $\sqcap$:

$$a \times (\sqcap i \in I \cdot a_i) = (\sqcap i \in I \cdot a \times a_i)$$

and
(3) infinite distributivity of multiplication over $\sqcup$:

$$a \times (\sqcup i \in I \cdot a_i) = (\sqcup i \in I \cdot a \times a_i).$$

Indeed, the complete distributivity between $\sqcap$ and $\sqcup$ properly describes interaction between angelic and demonic choices; and we even can say that the essence of the above theorem is three distributivities.

9 Conclusion

We employ a probabilistic logic as our logical tool for reasoning about probabilistic sequential programs. A probabilistic logic often provides us with a more precise description of probabilistic programs than classical two-valued logic used as a meta-logic in the previous works on probabilistic programming. We introduce the healthiness conditions of strong monotonicity, conjunctivity, disjunctivity and continuity, and a normal form theorem is established for each of them. The notions of probabilistic refinement and probabilistic correctness are introduced, and they are more delicate than the corresponding notions existing in the previous literatures. We give three probabilistic semantics to the contract language, namely, probabilistic predicate transformer semantics, probabilistic choice semantics, and probabilistic game semantics, and the relationship among them is clarified. In particular,

a probabilistic generalization of R. -J. Back and J. von Wright's winning strategy semantics is presented.

The constructs of recursion and iteration are not included in the proposed calculus. The reason is that some essential difficulties will arise when recursion and iteration are considered. Note that the operation that we use to combine probabilities of consecutive events is product. Thus, the limits of powers of certain reals, say a^n, will often be involved in the predicate transformer semantics of probabilistic recursive programs. Recall that in our setting, following [20, 21, 24, 25, 29], a probabilistic predicate is defined to be a bounded expectation function on the state space, and its values are allowed to exceed 1. However, the power a^n will approach infinity as n increases whenever a is greater than 1. This frequently makes the semantical function under consideration is not a probabilistic predicate transformer, violating the fundamental assumption of our semantics, since each probabilistic predicate is supposed to be bounded. A way to avoid this objection seems that we may restrict our attention on probabilistic predicates bounded by 1. It does enable us to escape from the difficulty of boundedness. Unfortunately, it still causes a certain difficulty, but at the other extreme. We observe that if a is less than 1, then a^n will vanish as n increases, and the probability information carried by a will be lost in the process of iteration.

The purpose of this paper is mainly to establish a mathematical foundation for probabilistic sequential programming. An very important problem for further development is to find some concrete applications which illustrate the power of the mathematical tools developed here.

In this paper, we only deal with angelic and demonic choices, leaving probabilistic choice ${}_p\oplus$ untouched. But as pointed out in [15, 24, 29], the probabilistic choice is at the heart of the theory of probabilistic programming. So, a unified treatment of probabilistic choice and angelic and demonic choices would be an interesting topic for further studies.

The theory developed in this paper enjoys another intuitive explanation except that of probabilistic (expectation) predicates. The new explanation is concerned with the price of computation, and in a sense the theory may be seen as a price-sensitive semantics of sequential programming. For example, in an angelic choice R, a decreasing function of $R.\sigma.\gamma$ may be thought as the price that the angel should pay to go from the initial state σ to the final state γ. Alternative interpretations of probabilistic (expectation) predicate would admit certain new operations, say minimum, to be used to replace product in the calculus developed in this paper. This may also allow us to cope with recursion and iteration in a much more smooth way. A refinement calculus based on a continuous-valued logic different from the probabilistic logic employed in the present paper should be another interesting topic for further studies.

Acknowledgements. The work reported in this paper was carried out when the author was visiting Turku Center for Computer Science, Data City, Lemminkäisenkatu 14A, FIN-20520 Turku, Finland. The author is very grateful to Professors Ralph-Johan Back and Joakim von Wright for their stimulating discussions and invaluable comments and suggestions and for providing the excellent working environment. The author also would like to thank the referees for their invaluable criticisms, comments and suggestions which helped to improve considerably the presentation of this paper. In particular, one of the referees kindly pointed out that the original version of Proposition 8(4) and its proof are wrong and provided the alternative proof of Proposition 27(3) in the Galois style.

References

1. S. Abramsky, R. Blute, P. Panangaden. Nuclear and trace ideals in tensor-* categories. Journal of Pure and Applied Algebra **143**, 3–47 (1999)
2. R. -J. Back, J. von Wright. A lattice-theoretical basis for a specification language. In: Mathematics of Program Construct, Groningen, the Netherlands, Lecture Notes in Computer Science 375. Springer-Verlag, 1989
3. R. -J. Back, J. von Wright. Duality in specification languages: a lattice-theoretical approach. Acta Informatica **27**, 583–625 (1990)
4. R. -J. Back, J. von Wright. Refinement Calculus: A Systematic Introduction. Springer-Verlag, New York 1998
5. J. Baeten, J. A. Bergstra, S. A. Smolka. Axiomatizing probabilistic processes: ACP with generative probability. Information and Computation **122**, 234–255 (1995)
6. J. A. Bergstra, J. -W. Klop. Algebra of communicating processes with abstraction. Theoretical Computer Science **33**, 77–121 (1985)
7. R. Carnap. Logical Foundations of Probability. University of Chicago Press, Chicago 1950
8. P. Cousot, R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In: Conference Record of the 4th ACM Symposium on Principles of Programming Languages, Los Angeles, CA, pp. 238-252, 1977
9. L. de Alfaro, R. Majumdar. Quantitative solution of omega-regular games. In: Proceedings of the 33th Annual ACM Symposium on Theory of Computing, STOC'01, Hersonissos, Crete, Greece, pp. 675-683, 2001
10. E. D. Dijkstra. Notes on structured programming. In: O. Dahl, E. W. Dijkstra, C. A. R. Hoare (eds.) Structured Programming. Academic Press, New York 1971
11. E. W. Dijkstra. A Discipline of Programming. Prentice Hall, Englewood Cliffs, NJ 1976
12. E. E. Doberkat. The converse of a probabilistic relation. Technical Report 113, University of Dortmund, 2001
13. E. E. Doberkat. The demonic product of probabilistic relations. Technical Report 116, University of Dortmund 2001.
14. J. Y. Halpern. An analysis of first-order logics of probability. Artificial Intelligence **46**, 311–350 (1990)
15. J. He, K. Seidel, A. K. McIver. Probabilistic models for the guarded command language. Science of Computer Programming **28**, 171–192 (1997)
16. W. H. Hesselink. Command algebras, recursion and program transformation. Formal Aspects of Computing **2**, 60–104 (1990)
17. C. A. R. Hoare. Communicating sequential processes. Communications of the ACM **21**, 666–677 (1978)

18. C. Jones. Probabilistic nondeterminism. Ph. D. thesis, Monograph ECS-LFCS-90-105, Edinburgh University, UK 1990
19. C. Jones, G. Plotkin. A probabilistic powerdomain of evalutions. In: Proceeding of the 4th IEEE Annual Symposium on Logic in Computer Science, pp. 186–195. Los Alamitos, California 1989
20. D. Kozen. Semantics of probabilistic programs. Journal of Computer and System Science **22**, 328–350 (1981)
21. D. Kozen. A probabilistic PDL. In: Proceedings of the 15th ACM Symposium on Theory of Computing, New York 1983
22. S. MacLane. Categories for the Working Mathematician. Springer, New York 1971
23. A. K. McIver, C. Morgan. Probabilistic power domains. Technical Report, Programming Research Group, Oxford University Computing Laboratory 1995
24. A. K. McIver, C. Morgan. Demonic, angelic and unbounded probabilistic choices in sequential programs. Acta Informatica **37**, 329–354 (2001)
25. A. K. McIver, C. Morgan. Partial correctness for probabilistic demonic programs. Theoretical Computer Science **266**, 513–541 (2001)
26. A. K. McIver, C. Morgan. Games, probability and the quantitative mu-calculus. In: M. Bazz, A. Voronkov (eds.) Logic for Programming, Artificial Intelligence, and Reasoning, pp. 292-310. 9th International Conference, LPAR'02. LNAI 2514, 2002
27. R. Milner. Communication and Concurrency. Prentice-Hall, Englewood Cliffs, NJ 1989
28. C. C. Morgan. Programming from Specifications. Prentice-Hall 1990
29. C. Morgan, A. McIver, K. Seidel. Probabilistic predicate transformers. ACM Trans. Programming Languages and Systems **18**, 325–353 (1996)
30. D. Monniaux. Abstract interpretation of probabilistic semantics. In: 7th International Static Analysis Symposium, SAS'00, LNCS 1824, Springer 2000
31. D. Monniaux. An abstract analysis of the probabilistic termination of programs. In: Static Analysis, 8th International Symposium, pp. 111-126. SAS'01, Paris, France, Proceedings, LNCS 2126, Springer 2001
32. N. Nilsson. Probabilistic logic. Artificial Intelligence **28**, 71–88 (1986)
33. P. Panangaden. Probabilistic relations. In: C. Baier, M. Huth, M. Kwiatkowska, M. Ryan (eds.) PROBMIV'98, pp. 59–74. 1998
34. J. Pearl. Probabilistic Reasoning in Intelligent Systems. Morgan-Kaufmann 1988
35. G. D. Plotkin. A Structured Approach to Operational Semantics. Report DAIMI FN-19, Aarhus University 1981
36. T. Raghavan, J. Filar. Algorithms for stochastic games - a survey. ZOR - Methods and Models of Operational Research **35**, 437–472 (1991)
37. H. Reichenbach. Wahrscheinlichkeitslogik. *Erkenntnis* **5**, 37–43 (1835–36)
38. N. Rescher. Many-Valued Logic. McGraw-Hill, New York 1969
39. K. Seidel. Probabilistic communicating processes. *Theoretical Computer Science* **152**, 219–249 (1995)
40. L. Shapley. Stochastic games. Proc. Nat. Acad. Sci. USA **39**, 1195–1100 (1953)
41. F. van Breugel, J. Worrell. Towards quantitative verification of probabilistic transition systems. In: F. Orejas, P.G. Spirakis, J. van Leeuwen (eds.) Proceedings of the 28th International Colloquium on Automata, Languages, and Programming (ICALP), Crete, July 2001, Lecture Notes in Computer Science 2076, Springer-Verlag, pp. 421–432
42. F. van Breugel, J. Worrell. An algorithm for quantitative verification of probabilistic transition systems. In: K.G. Larsen, M. Nielsen (eds.) Proceedings of the 12th International Conference on Concurrency Theory (CONCUR), Aalborg, August 2001, Lecture Notes in Computer Science 2154, Springer-Verlag, pp. 336–350
43. R. J. van Glabbeek, S. A. Smolka, B. Steffen. Reactive, generative, and stratified models of processes. Information and Computation **121**, 59–80 (1995)

44. N. Wirth. Program development by stepwise refinement. Communications of the ACM **14**, 221–227 (1971)
45. J. von Wright. The lattice of data refinement. Acta Informatica **31**, 105–135 (1994)
46. M. S. Ying. Topology in Process Calculus: Approximate Correctness and Infinite Evolution of Concurrent Programs. Springer-Verlag, New York 2001
47. M. S. Ying. Bisimulation indexes and their applications. Theoretical Computer Science **275**, 1–68 (2002)
48. M. S. Ying. Additive models of probabilistic processes. Theoretical Computer Science **275**, 481–519 (2002)
49. M. S. Ying, M. Wirsing. Approximate bisimilarity. In: T. Rus (ed.) Algebraic Methodology and Software Technology, 8th International Conference, AMAST 2000, Iowa City, USA, May 20-27, 2000, Proceeedings, Lecture Notes in Computer Science 1816, Springer-Verlag, pp. 309–321
50. Z. Zawirski. Znaczenie logiki wielowartosciowej dla poznania i zwiqzek jej z rachunkiem prawdopodobienstwa. Przeglad Filozoficzny **37**, 393–398 (1934)